LAUREA

Mobiilitietoturvan kehittäminen Halti Oy:ssä ohjeiston avulla

Hyyryläinen, Olli

2011 Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Mobiilitietoturvan kehittäminen Halti Oy:ssä ohjeiston avulla

Hyyryläinen, Olli
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Marraskuu, 2011

Laurea-ammattikorkeakoulu **Tiivistelmä**
Laurea Leppävaara
Tietojenkäsittelyn koulutusohjelma

Hyyryläinen, Olli

Mobiilitietoturvan kehittäminen Halti Oy:ssä ohjeiston avulla

Vuosi 2011 Sivumäärä 44

Mobiililaitteista älypuhelimien ja sormitietokoneiden määrä on kasvanut räjähdysmäisesti viimeisen viiden vuoden aikana. Perinteisten matkapuhelintenkin ominaisuudet ovat kehittyneet siihen pisteeseen, että matkapuhelimia on jo vaikeaa luokitella niihin, jotka ovat tai eivät ole älypuhelimia. Yrityksissä kehitys on huomattu, ja entistä useammalla työntekijällä on käytössään älypuhelin laajakaistanopeuteen kykeneväksi mainostetulla langattomalla tiedonsiirtoyhteydellä. Internet on työntekijää lähempänä kuin koskaan aikaisemmin.

Nopealla informaatio- ja kommunikaatioteknologian kehityksellä on haittapuolensa; älypuhelimet kykenevät tehtäviin joihin aikaisemmin tarvittiin kannettavia tietokoneita, mutta laitteiden valmistajat ja käyttäjät eivät välttämättä osaa suhtautua tähän tosiasiaan. Tämä lisää tietoturvallisuuteen liittyviä riskejä. Tietoturvaa eivät myöskään edistä kasvavasti mobiililaitteilla käytetyt sosiaalisen median palvelut. Sosiaalinen media, nk. some, mahdollistaa yrityksille uudenlaisia keinoja tavoittaa asiakkaansa, mutta se mahdollistaa myös uudenlaisia keinoja menettää asiakkaita ja työntekijöitä. Mobiililaitteita ja sosiaalista mediaa koskevat tietoturvauhat limittyvät niin kriittisesti, että someen liittyviä uhkia käsitellään tässä opinnäytetyössä myös mobiililaitteiden uhkina.

Monilla yrityksillä ei ole selkeätä ohjeistoa, jossa käsiteltäisiin mobiililaitteisiin ja sosiaaliseen mediaan liittyviä kysymyksiä. Tässä opinnäytetyössä kehitetään konstruktiivisella tutkimuksella molemmat aiheet kattava ohjeisto suomalaiselle ulkoiluvarusteyritys Halti Oy:lle yrityksen toimeksiannosta. Tutkimus perustuu pitkälti Järvisen ja Järvisen Tutkimustyön metodeista kirjan antamiin metodi artefaktin konstruoimisen ohjeisiin ja Suomen Valtionhallinnon tietoturvallisuuden johtoryhmän tietoturva-aiheiseen kirjallisuuteen.

Tutkimuksen lopputuloksena saadun ohjeiston avulla Halti Oy voi turvata matka- ja älypuhelimiensa tietoturvan yritykselle järkevällä tavalla. Tulevaisuudessa ohjeisto täytyy kehittää vastaamaan tulevia uhkia ja mahdollisuuksia, joita kehittyvä teknologia luo jatkuvasti.

Asiasana mobiililaitteet, tietoturva, ohjeisto

University of Applied Sciences **Abstract**
Laurea Leppävaara
Bachelor's Degree Programme in Business Information Technology

Hyyryläinen, Olli

The development of mobile information security by guidelines in Halti Oy

Year 2011 Pages 44

Smartphone and tablet computer mobile devices have experienced an explosive growth in sales during the last five years. The so called traditional mobile phones and feature phones have progressed so far in technology that it is actually hard to classify what is and what isn't a smartphone. Business organizations have observed this progress of technology and so more and more employees carry smarphones equipped with wireless Internet connections advertised to reach broadband speeds. The Internet is closer to the employee than ever before.

The rapid development of information and communication technology has its downsides: smartphones are able to do perform which used to need laptops so manufacturers and consumers do not necessarily know how to face with this fact. This increases information security risks. The information security is not furthered by increasing use of social media services on mobile devices. Social media enable businesses new ways to reach their clientele but they also enable new ways to lose clientele and employees. Information security risks concerning mobile devices and social media are so intertwined that this thesis considers the risks of social media to be part of the information security of mobile devices.

Many businesses do not have clear guidelines concerning questions raised by mobile devices and social media. This thesis develops guidelines to aforementioned subjects using constructive research for Finnish outdoor sports and recreation equipment manufacturer Halti by the authorization of the company. Research process is based largely on method artifact construction guidelines provided by book Tutkimustyön metodeista by Järvinen and Järvinen.

Halti Oy can use the guidelines created by the research to reasonably protect its traditional phones and smartphones. In the future the guidelines must be developed to respond to threats and opportunities which constantly progressing technology creates.

Keywords mobile devices, information security, guidelines

Sisällys

1 Johdanto

Housujen taskussa kannettavien tietokoneiden aika on nyt. Vuodesta 1990, jolloin 12 miljoonalla ihmisellä maailmassa oli suuri, kallis ja huonosti toimiva matkapuhelin, esimerkiksi Suomen kansakunta on päässyt tilanteeseen, jossa joka neljännellä suomalaisella 15–79-vuotiaalla on käytössään mukana kuljetettavan puhelimen ja tietokoneen risteytys: älypuhelin (Cellullar Subscribers 1990 2004; Leino 2011). Halvimmat vuonna 2011 valmistetut älypuhelimet voittavat täysin vuoden 1990 monikymmenkertaisesti isommat kuluttajille tarkoitetut pöytätietokoneet niin hinnallaan, kuin teknisillä ominaisuuksillaan. Kalliimpia älypuhelimia voidaan verrata jo muutaman vuoden takaisiin halvemman luokan tietokoneisiin (Waisybabu 2011). Informaatio- ja kommunikaatioteknologiaan erikoistunut tutkimus- ja tiedotusyritys Gartner ennustaa älypuhelimien myynnin ohittavan pöytätietokoneiden myynnin vuonna 2013 (Smartphone malware 2011, 11).

Tämän opinnäytetyön tarkoituksena on tuoda esiin ja kehittää asiakasyritys Halti Oy:n mobiililaitteiden tietoturvaa muokkaamalla sen työntekijöille selkeä kronologinen ohjeisto, jota noudattamalla turvataan yrityksen mobiilitietoturva sille järkevällä tavalla. Liitteenä oleva ohjeisto on kaksiosainen: ensimmäinen osa on tarkoitettu yrityksen IT-osastolle ja toinen mobiililaitteiden käyttäjille. Ensimmäinen osa koostuu askelista, jotka IT-osaston täytyy suorittaa ennen uuden mobiililaitteen käyttöönottoa ja asioista, joita täytyy valvoa laitteen ollessa käytössä ja lopuksi hävitettäessä se. Toinen osa, joka on vähemmän askellettu, kertoo käyttäjille mitä heidän tulee tietää mobiililaitteensa tietoturvasta, ja mitä sillä saa ja ei saa tehdä. Käyttäjän ohjeita varten opinnäytetyössä käsitellään myös sosiaalista mediaa, sillä siihen liittyvät palvelut ovat nousseet yksiksi käytetyimmistä, puhutuimmista ja riskialttiimmista jatkuvasti mukana kulkevan Internetin osista. Tietoturvaohjeiston pohjana käytetään vanhoja sekä uusia ohjeistoja ja ohjeita. Näitä vertaillaan toisiinsa, Halti Oy:n tarpeisiin, sekä artikkeleihin jotka käsittelevät ohjeistojen puutteita. Perusteluja ohjeiston luomiselle ja sen aiheille käsitellään luvuissa ”1.2 Halti Oy toimintaympäristönä” ja ”3. Uuden metodin kehittely”. Halti Oy:llä ei ole tällä hetkellä aikeita hankkia kämmen- eikä sormitietokoneita tulevaisuudessa, joten opinnäytetyö keskittyy matka- ja älypuhelimien tietoturvaan. Toimeksianto konstruktiiviseen tutkimukseen syntyi työharjoittelun aikana asiakasyrityksen toimesta, kun se ilmaisi huolensa laitteistonsa tietoturvasta. Neuvonpidossa todettiin tietoturvan olevan kauttaaltaan ajankohtainen aihe yritykselle ja rajauksen vuoksi tietoturvaa sovittiin käsiteltävän mobiililaitteiden näkökulmasta. Halti osakeyhtiötä toimintaympäristönä käsitellään luvussa ”1.2 Halti Oy toimintaympäristönä”, jossa pohditaan myös Halti Oy:n mobiilitietoturvan tilaa nyt ja sitä, miksi ja miten tietoturvaa tarvitsee kehittää.

Opinnäytetyö seuraa Järvisen ja Järvisen Tutkimustyön metodeista – kirjassa (2004, 103–117) annettuja suuntaviivoja konstruktiivisen tutkimuksen metodi -artefaktin konstruoimiselle. Opinnäytetyössä seurataan metodin ja realisoinnin toteutusta, muttei metodin käyttöä ja ylläpitoa tai metodin hävittämistä. Nämä askeleet jätetään asiakasyrityksen kanssa pidetyn neuvonpidon mukaisesti heille. Opinnäytetyöprosessissa on noudatettu osaltaan myös Ojasalon, Moilasen ja Rintalahden Kehittämistyön menetelmät – kirjan (2009, 67) konstruktiivisen prosessin vaiheita. Ohjeiden, prosessien ja hyvän tieteellisen tavan noudattaminen ja sisäistäminen tuodaan esiin opinnäytetyön rakenteessa, sisällössä ja oikeellisuudessa.

Primäärilähteinä työssä on pyritty käyttämään ensisijaisesti uusia mobiililaitteista, tietoturvasta, sosiaalisesta mediasta ja muista tärkeistä aiheista kertovia tutkimuksia, kirjoja, sekä sähköisiä ja perinteisiä artikkeleita. Tutkimukset ovat olleet lähteinä tärkeysjärjestyksessä korkeimmalla, mutta mikäli uudempia uutisartikkeleita aiheesta on tullut, ovat ne olleet etusijalla. Primäärilähteet on seulottu niiden relevanttiuden, luotettavuuden ja tuoreuden perusteella. Mobiililaitteisiin liittyvän tiedon hajanaisen luonteen vuoksi, on tietoa jouduttu keräämään monien eri uutissivustojen, yritysten ja yhteisöjen verkkosivustoilta. Opinnäytetyössä esiintyviin kuviin on pyydetty käyttöoikeus niiltä järjestöiltä joihin on saatu yhteys, ja työssä on pyritty välttämään yksityisten yritysten tuottamaa visuaalista materiaalia. Materiaalia, jonka kopioiminen on selkeästi kielletty, ei ole käytetty ollenkaan. Tiedonhankinnan lisäksi, opinnäytetyö perustuu pitkälti Stakesin Kehittämistyön menetelmät tutkielmassa (2006, 8) määriteltyyn havainnointiin ja toimeksiantajayrityksen yhteyshenkilöiden kanssa käytyyn suunnittelupaja tyyppiseen keskusteluun. Havainnointi katsottiin päteväksi tiedonkeruumenetelmäksi, koska opinnäytetyön tekijä työskenteli viiden kuukauden mittaisessa työharjoittelussaan Halti Oy:n IT-osastolla joka on vastuussa yrityksen mobiilitietoturvasta ja tietoteknisestä laitteistosta. Toimeksiantajayrityksen yhteyshenkilöiden kanssa käyty keskustelu on pitkälti koostunut epämuodollisista kasvokkain käydyistä palavereista, joissa opinnäytetyötä on muotoiltu, terävöitetty ja ohjattu Halti Oy:lle sopivaan suuntaan. Opinnäytetyössä pyritään selvästi erottamaan sen tekijän ja kirjallisen lähdemateriaalin tiedot ja mielipiteet.

Työn luvut etenevät sovelletusti Järvisen ja Järvisen (2004, 117) esittelemän metodi artefaktin konstruoimiseen tarkoitetun tutkimuksen sisällysluettelon perusteella. Ensimmäinen luku esittelee opinnäytetyön ja avaa siihen liittyvät keskeiset käsitteet. Toinen luku kertoo aikaisemmista mobiilitietoturvaa koskevista metodeista ja esittelee niihin parannuksia. Kolmannessa luvussa edetään Halti Oy:lle sopivan metodin rakentamiseen aikaisempien ohjeistojen, Halti Oy:n tarpeiden ja tulevaisuuden uhkien pohjalta. Neljäs luku käsittelee opinnäytetyön prosessia ja sen tuloksia.

1.1 Keskeinen terminologia

Tässä luvussa käsitellään opinnäytetyön keskeistä terminologiaa ja avataan hieman termeihin liittyviä aiheita. Aiheiden avaamisen tarkoituksena on antaa opinnäytetyölle tausta, kertoa mobiililaitteisiin liittyvistä keskeisistä teknologioista ja helpottaa näin termistön ymmärtämistä. Viimeistään tämän luvun lukemisen jälkeen lukijan tulisi ymmärtää esimerkiksi mitä laitteita tarkoitetaan mobiililaitteilla, mitä tarkoitetaan eri matkapuhelinverkkosukupolvilla, mitkä ovat suosituimmat mobiilikäyttöjärjestelmät, mitä eri yhtiöiden sovelluskaupat ovat ja mitä mobiilitietoturva oikein tarkoittaa. Mobiilitietoturvaa käsitellessä täytyy ymmärtää mitä mobiili ja mobiililaite – sanoilla tarkoitetaan. Seuraavassa käydään hieman läpi niiden tarkoitusta yleisesti ja sitä, mihin niillä viitataan opinnäytetyössä.

Kolumnisti ja konsultti Jukka Korpisen laatima Pienehkö sivistyssanakirja (2008), sivistyssanoihin erikoistunut verkkosivusto, määrittelee mobiili – sanan tarkoittamaan matkapuhelinta, kännykkää tai muuta matkaviestintä, mutta korostaa myös, ettei sanalle ole tässä tarkoituksessa kovin hyvää suomalaisempaa vastinetta. Sanaa voidaan käyttää myös adjektiivina ja etuliitteenä tarkoittaen liikkuvaa, liikuteltavaa, siirrettävää, langatonta. ”Mobiilius” viittaa Korpisen mukaan nykyisin usein olennaisesti vain tiedonsiirron langattomuuteen, esimerkkinä mobiiliverkko eli matkapuhelinverkko. MOT-sanakirja suomentaa englanninkielisen ”mobile” –sanan tarkoittaman samaa: matkapuhelinta, kännykää, siirrettävää, siirreltävää, liikuteltavaa. Suomeksi sanakirja selittää mobiili –sanan pelkästään adjektiiviksi. Opinnäytetyössä mobiili –sanaa käytetään pelkästään etuliitteenä ja adjektiivina.

Oxfordin edistyneen oppijan tietosanakirja –verkkosivusto (2011) määrittelee mobiililaitteeksi minkä tahansa pienen tietojenkäsittelyyn soveltuvan tietoteknisen laitteen, joka mahtuu taskuun. Tietosanakirja antaa esimerkeiksi kämmentietokoneen (PDA) ja älypuhelimen. Käytettävyyden tutkijat Gorlenko ja Merrick (2003, 641) ovat sitä mieltä, että mobiilaite on laite, jota käytettäessä sitä ei tarvitse laskea millekään alustalle. Kannettava tietokone ei esimerkiksi täytä tätä määritelmää, koska se on käyttöä varten käytännössä aina laskettava syliin, pöydälle tai muulle alustalle. Määritelmiä seuraamalla mobiililaitteita ovat siis esimerkiksi kämmentietokoneet, käsipelikonsolit, digitaaliset kamerat, digitaaliset ääninauhurit, digitaaliset laskimet, mp3-soittimet, e-kirjalukijat, navigaatiolaitteet, hakulaitteet, langattomat puhelimet, sormitietokoneet, matkapuhelimet ja älypuhelimet. Opinnäytetyön rajaamiseksi Halti Oy:lle ajankohtaiseksi todettuihin aiheisiin, tässä työssä mobiililaite –sanalla viitataan vain matkapuhelimiin ja älypuhelimiin, ellei asiayhteydessä muuta anneta ymmärtää.

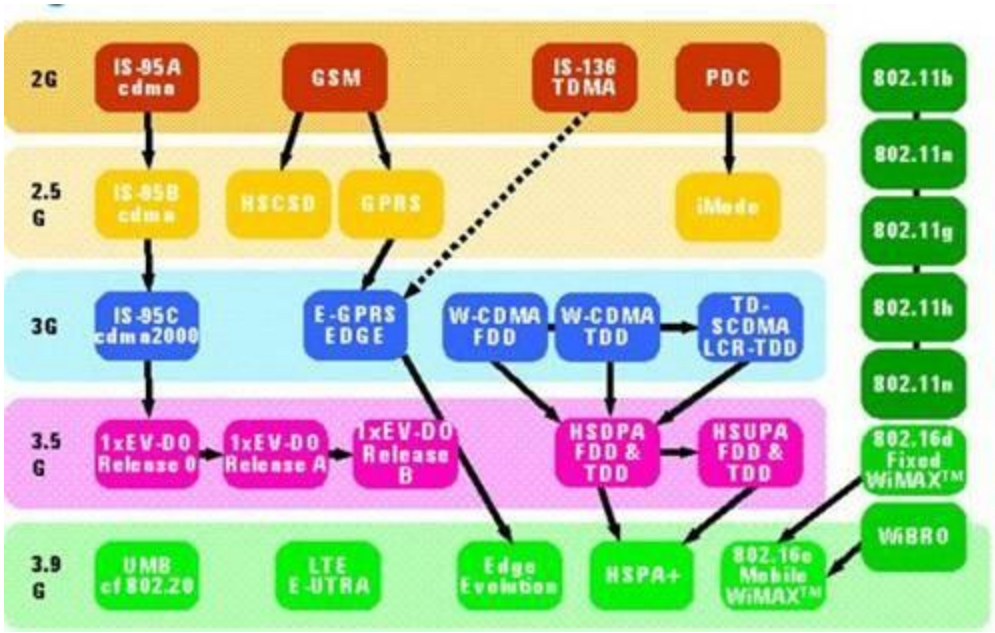
Matkapuhelimien ja älypuhelimien välinen ero on hyvä määritellä, koska senkin tulkinnassa on eroja. Steve Litchfield keskustelee allaboutsymbian.com, suurimmalla Symbian OS mobiilikäyttöjärjestelmään keskittyneellä verkkosivustolla, kirjoittamassaan artikkelissa Defining Smartphone (2010) siitä miten älypuhelin pitäisi määritellä, miten moni määritelmä pätee nykyisin normaaleiksi matkapuhelimiksi kutsuttuihin laitteisiin ja pitäisikö älypuhelin ja matkapuhelin edes määritellä eri tavoin. Litchfieldin johtopäätös on, että matkapuhelimet ja älypuhelimet täytyy määritellä eri laitteiksi ja summaa älypuhelimen määritelmäksi seuraavan: älypuhelin käyttää uusille sovelluksille avointa käyttöjärjestelmää ja on pysyvästi yhdistettynä Internetiin. Vaikka Litchfield itsekin toteaa määritelmän olevan epätäydellinen, on se opinnäytetyötä varten riittävä Halti Oy:n laitteisto huomioon ottaen. Kuriositeettina mainittakoon, että Nokian Communicator 9000:n vuodelta 1996 katsotaan olevan ensimmäinen laajalle levinnyt älypuhelin, jonka huonoiksi puoliksi eräs arvostelu mainitsee hankalan käyttöliittymän ja suppean sovellusvalikoiman (Catanzariti 2009; Uusheimo 1998).

Esimerkiksi älypuhelimilla tapahtuvan Internetin selaamisen mahdollistava langaton tiedonsiirto on aiheena laaja ja monimuotoinen. Se on perustunut ihmiskunnan historiassa viimeistä paria sataa vuotta lukuun ottamatta pelkästään ääneen ja visuaalisiin merkkeihin. Seuraavassa käydään lyhyesti läpi Patil ym. (2003) keräämää materiaalia langattomasta tiedonsiirrosta, koska tämän teknologian kehittyminen on alun perin mahdollistanut matkapuhelimet. Nykyisin elektronisen laitteiston välityksellä käytävä langaton tiedonsiirto perustuu sähkömagneettiseen säteilyyn tietyillä taajuusalueilla, kuten esimerkiksi puhelimien käyttämiin radioaaltoihin. Radioaallot ovat jaettu taajuusalueensa perusteella erilaisia tehtäviä varten. Tietyt taajuudet sopivat tiettyihin tehtäviin riippuen siitä kuinka pitkälle ne kantavat, kuinka paljon niiden tiedonsiirtokapasiteetti on ja kuinka hyvin ne kulkeutuvat erilaisissa olosuhteissa. Näiltä ominaisuuksiltaan esimerkiksi puhelimien tarpeisiin optimaaliset taajuudet ovat jaettu ja luokiteltu tarkasti, koska käytännöllisiä taajuuksia on vain rajallinen määrä. Taajuuksien rajallisuus on johtanut niistä saatavan hyödyn jatkuvaan kehittämiseen.

Puhuttaessa matkapuhelinverkkojen sukupolvista, viitataan erilaisilla sopimuksilla määriteltyihin teknisiin määreisiin ja teknologioihin, jotka määrittelevät lähinnä sen millä, miten ja mitä radioaaltotaajuuksia käytetään hyväksi. On tärkeää huomioida ettei sukupolvien vaihtuminen ole pakollisesti poistanut vanhempiin sukupolviin liittyvää teknologiaa käytöstä. Ensimmäinen matkapuhelinverkkosukupolvi (1G) kehitettiin 1970-luvulla. Se oli analoginen ja suunniteltu vain puheen välittämiseen matkapuhelinten välillä. Toisen sukupolven (2G) verkot siirtyivät Euroopassa analogisista järjestelmistä, kuten NMT:stä, yhtenäisempään digitaaliseen Global System for Mobile Communication (GSM) järjestelmään.

General Packet Radio Service (GPRS) on GSM verkon parannus, jolla saatiin tehostettua verkon käyttöä. Kolmannen matkapuhelinverkkosukupolven (3G) kehittäminen aloitettiin jo 1980-luvun lopulla ja esiteltiin vuonna 1992 ITU World Radio konferenssissa. Sen mukanaan tuomana suurimpana muutoksena voidaan katsoa olleen pakettipohjaisten palveluiden mahdollistaminen matkapuhelinverkoissa. Näin mahdollistettiin myös Internetin sujuva selaaminen matkapuhelimilla.

Ensimmäisen ja toisen sukupolven välinen ero matkapuhelinverkoissa on selkeä, vaihdos analogisuudesta digitaalisuuteen. Toisen, kolmannen ja varsinkin neljännen sukupolven väliset erot eivät ole aivan yhtä selkeitä. Yhdistyneiden Kansakuntien perustaman informaatio- ja kommunikaatioteknologia järjestö International Telecommunication Unionin (ITU) (2009, 2) mukaan suurin osa käytössä olevasta kolmannen sukupolven, niin kutsutun IMT-2000 standardiperheen, matkapuhelinverkkojen teknologiasta perustuu 2G:ssä määriteltyjen teknologioiden parannuksiin. Valmiina olevan teknologian parannus on ollut monille operaattoreille uuteen teknologiaan siirtymistä helpompaa. Ilmeisesti operaattoreilla on kiire siirtyä neljänteen sukupolveen, sillä jotkin niistä ovat alkaneet nimittää IMT-2000 standardiperheen teknologioiden parannuksia 4G:ksi, vaikka parannukset eivät kuulu ITU:n määrittelemään seuraavan sukupolven IMT-Advanced standardiperheeseen. ITU:n (2009, 3) mukaan 3G:n kehittämisellä on vielä suurta potentiaalia joka täytyy hyödyntää ennen 4G:hen kiirehtimistä. Kolmannen sukupolven matkapuhelinverkkojen niin kutsuttuihin laajakaistanopeuksiin kykenevän langattoman tiedonsiirron yleistymisen voidaan katsoa olevan yksi älypuhelimien suosion kasvun syistä maailmalla (Claro Brazil keeps the customer satisfied with 3G 2010; Domestic Manufacturers Cashing in on Smartphone Popularity 2011). Kuvan 1 on tarkoitus hahmottaa eri langattomien teknologioiden kehittymistä siirryttäessä 1G:stä ”3,9G:hen”. On tärkeätä ottaa huomioon, että esimerkiksi kuvan 802.11x –standardit ovat lähiverkkojen langattomaan tiedonsiirtoon tarkoitettuja.



Kuva 1: Langattomaan tiedonsiirtoon kehitettyjen teknologioiden sukupolvet matkapuhelinten näkökulmasta (International Telecommunication Union 2008)

Aiemmin luvussa älypuhelimien määritelmässä esiintynyttä termiä ”uusille sovelluksille avoimet käyttöjärjestelmät” on tärkeää tarkastella lähemmin, koska se on Halti Oy:n, sekä kaikkien maailman mobiililaitteiden tietoturvalle olennaista. Seuraavassa esitettyjen tilastoiden pitäisi olla tarkkoja, mutta lukijan on vastaisuudessa syytä huomioida että eri lähteissä esitettyjen tilastojen prosentit ja myyntiluvut voivat vaihdella, riippuen siitä miten älypuhelin niissä määritellään. Huomiota tulee kiinnittää myös siihen koskevatko tilastot matkapuhelimia, älypuhelimia vai kaikkia mobiililaitteita, ja perustuvatko tilastot sen hetkisiin myyntimääriin vai ylipäätään laitteiden käytön määrään. Tällä hetkellä markkinoiden tärkeimmät älypuhelimien käyttöjärjestelmät ovat markkinaosuuksiensa perusteella Applen iOS, Googlen Android, Nokian hylkäämä SymbianOS ja Research In Motionin (RIM) BlackBerry OS. Matkapuhelimien, älypuhelimien ja sormitietokoneiden käyttöjärjestelmiä tarkastellessa kaikkiansa Applen iOS hallitsee markkinoita 61,5 prosentin markkinaosuudella, Android tulee toisena 18,9 % osuudella, kolmantena tavallisissa matkapuhelimissa suosittu Java ME 12,8 % osuudella, neljäntenä SymbianOS 3,5 %:lla ja viidentenä BlackBerry OS 2,5 %:lla (Mobile/Tablet Top Operating System Share Trend 2011).

Opinnäytetyön tekijän mielestä tulevaisuudessa on hyvä kiinnittää huomiota onnistuvatko älypuhelimiin tarkoitettu Microsoftin Windows Phone 7 ja sormitietokoneillekin tuleva Windows 8:n valtaamaan markkinoita. Tietoviikko –uutissivuston toimittaja Niko Rinta (2011) pitää Microsoftin Windows Phone 7 –mobiilikäyttöjärjestelmän tietoturvaa sille mahdollisena myyntivalttina. Toimittaja kirjoittaa, että jos Microsoft onnistuu luomaan tietoturvallisen sovellusympäristön ja jakelukanavan yrityssovelluksille, on sillä mahdollisuus menestyä. Rinta suhtautuu asiaan kuitenkin varauksella, sillä Microsoftilla on pitkä historia huonosta tietoturvasta.

Edellä mainitut mobiilikäyttöjärjestelmät mahdollistavat erilaisia tietoturvaan liittyviä teknisiä ratkaisuja estämään joidenkin tietoturvauhkien toteutumista. Halti Oy:n käyttämistä mobiilikäyttöjärjestelmistä enemmän luvussa ”1.2 Halti Oy toimintaympäristönä”. Käyttöjärjestelmien tietoturvan kannalta on tärkeää huomioida, että espanjalaisen The National Cyber-Security Advisory Council (CNCCS) (Smartphone Malware 2011, 24), tästä lähtien opinnäytetyössä CNCCS, tietoturvajärjestön mukaan vuoteen 2011 tullessa lähes kaikki mobiilihaittaohjelmat ovat suuntautuneet vain Nokian vahvasti käyttämää SymbianOS -mobiilikäyttöjärjestelmää vastaan. iPhonen ja Google Android –mobiilikäyttöjärjestelmän suosion ja Symbianin lakkauttamisen myötä haittaohjelmien pääasiallinen kohde siirtyy CNCCS:n mukaan luultavasti näihin uudempiin mobiilikäyttöjärjestelmiin. Seuraavassa esitellään lyhyesti järjestyksessä iOS, Android, Java ME, SymbianOS ja BlackBerry OS käyttöjärjestelmät, koska ne eroavat ominaisuuksiltaan, yhtiöidensä politiikoilta ja tietoturvaltaan. Tietoturvaominaisuuksiin palataan luvuissa ”2.1 Aikaisemmat mobiilitietoturvaa koskevat metodit”. SymbianOS:sää käsitellään vielä edellä mainitun luvun lisäksi luvuissa ”1.2 Halti Oy toimintaympäristönä” ja ”3.1 Uuden metodin kehittely”.

Amerikkalaisen elektroniikkayritys Applen kehittämä mobiilikäyttöjärjestelmä iOS on selkeästi markkinoiden tämän hetken suosituin käyttöjärjestelmä sekä älypuhelimissa, että sormitietokoneissa (Mobile/Tablet Top Operating System Share Trend 2011). Applen viralliselta Internet-sivustolta on nähtävissä, että iOS käyttöjärjestelmä esiintyy myös multimediaan erikoistuneessa iPod touch -mobiililaitteessa (iPod touch, 2011). Dwivedi, Clark ja Thiel (2010, 50) kirjoittavat että Applen iPhone -älypuhelin yllätti markkinat hienostuneisuudellaan ja sai muutkin kuin yrityskäyttäjät kiinnostumaan älypuhelimista tullessaan myyntiin vuonna 2007.

2008 vuoden heinäkuussa Apple julkaisi maailman ensimmäisen keskitetyn mobiilisovelluksia tarjoavan verkkokaupan: App Storen. Tänä päivänä App Store tarjoaa yli 500000 sovellusta, jotka Apple tarkistaa niiden haitallisuuden varalta ennen kuluttajille julkaisemista (From the App Store; Smartphone Malware 2011, 15). CNCCS:n (Smartphone Malware 2011, 15) mukaan Apple myös vaatii kaikkia sovelluskehittäjiä rekisteröitymään ja maksamaan kausittaista maksua. Vaikka sovellukset tarkastetaan etukäteen, myös iPhonelle on olemassa haittasovelluksia. Ensimmäinen iPhone mato ilmestyi vuonna 2009 ja vaihtoi saastutetun laitteen taustakuvan poplaulaja Rick Astleyksi (Smartphone Malware 2011, 23). iPhonen sovellukset ohjelmoidaan Objective-C –ohjelmointikielellä.

Dwivedi, Clark ja Thiel (2010, 16) kertovat että Androidin on kehittänyt Googlen perustama Open Handset Alliance. Dwivedin ym. (2010, 16) mukaan Android perustuu Linuxin käyttöjärjestelmäytimeen ja sen sovellukset suurimmaksi osaksi Java -ohjelmointikieleen. Androidin tietoturvamalli perustuu suoraan Linuxin käyttöjärjestelmäytimeen. Androidista puhutaan avoimena käyttöjärjestelmänä, koska sovelluskehittäjät voivat tehdä sille uusia sovelluksia ja nähdä ja muokata Androidin lähdekoodia ilmaiseksi. CNCCS:n (Smartphone Malware 2011, 15) mukaan Googlen tuottamaan Adroidin sovelluskauppaan, Android Markettiin, saa rekisteröitymisen jälkeen kuka tahansa ladata omatekemän sovelluksensa ja jättää mobiililaitteen tietoturvan käyttäjän hyväksyttäväksi. Google kuitenkin poistaa haitallisiksi todetut ohjelmat niiden paljastumisen jälkeen. Tämä strategia ei ole toiminut ilmeisen hyvin, sillä Kotilaisen (2011) artikkelin mukaan Android Marketissa olevien haittasovellusten määrä on kasvanut 472 prosenttia heinäkuu-marraskuu 2011 välisenä aikana. Kotilaisen lainaamat tilastot kertovat, että 55 prosenttia näistä haittasovelluksista on käyttäjän tietoja varastavia troijalaisia ja 44 prosenttia tekstiviestejä maksullisiin numeroihin lähettäviä troijalaisia. Tutkimus- ja tiedotusyritys Gartner (2011) kertoo Androidia käyttävien älypuhelimien myynnin olevan 2011 vuoden kolmannella kvartaalilla jo 52,5 % kaikkien älypuhelimien myynnistä.

Teknologiayritys Oraclen (2011) mukaan sen omistamaa Java -ohjelmointikieltä käytetään yli kolmessa miljardissa matkapuhelimessa ympäri maailman. Netmarketshare (2011) tilastointiyritys tarkentaa, että Java Platform, Micro Edition (Java ME) –versiota Java –ohjelmointikielestä käyttöjärjestelmänään käyttävien puhelimien osuus kaikista matkapuhelimista ja älypuhelimista on 12.8%. Mobiilikäyttöjärjestelmänä Java ME on siitä poikkeuksellinen, ettei se Dwivedin ym. (2010, 152) mukaan ole täysi käyttöjärjestelmä, vaan kokoelma standardeja, joita noudattamalla halukkaat operaattorit ja laitevalmistajat saavat Java ME:n toimimaan laitteissaan, kuten Blu-Ray –soittimissa, printtereissä, televisioissa ja monissa muissa. Java ME:tä omissa laitteissansa lisenssillä käyttäviä valmistajia ovat mm. Ericsson AB, IBM, LG Electronics, Siemens AG ja Nokia.

Opinnäytetyöntekijä haluaa huomauttaa, että mikäli edellisissä osioissa mainitut prosentuaaliset markkinaosuudet laajennettaisiin koskemaan kaikkia elektronisia laitteita, Oracle luultavasti johtaisi tätä tilastoa ylivoimaisesti. Oracle (2011) toimittaa halukkaille työkalut sovelluksien luomiseen Java ME:llä ja mainostaa että Java ME:llä ohjelmoituja sovelluksia on kymmeniä tuhansia, muttei ohjaa verkkosivustoillaan ihmisiä mihinkään sovelluskauppoihin. CNCCS (Smartphone Malware 2011, 24) pitää huomioimisen arvoisena haittaohjelmien viime vuosien jatkuvaa lisääntymistä Java ME:tä tukeviin laitteisiin.

Vaikka hieman aiemmin todettiin Nokian käyttämän SymbianOS:n markkinaosuuden olevan matkapuhelimien, älypuhelimien ja sormitietokoneiden myynnissä vain 3,5 prosenttia, on sen osuus CNCCS:n (Smartphone Malware 2011, 10) vain älypuhelimien käyttöön keskittyneissä tilastoissa tänä vuonna spekulatiivisesti vieläkin suurin: 34 prosenttia. Dwivedi ym. (2010, 182) osoittavat, että termi ”Nokian SymbianOS” –käyttöjärjestelmä on periaatteessa väärä, sillä käyttöjärjestelmän loi alun perin Psion ja vuonna 1998 SymbianOS:n kehitys siirrettiin Psionin, Nokian, Motorolan, Ericssonin ja NTT DoCoMon perustaman Symbian Ltd.:n haltuun. Tänä päivänä Symbian -tavaramerkki on Symbian Foundation Ltd.:n hallussa, joka vuonna 2010 julkaisi Symbianin lähdekoodin jaettavaksi ilmaiseksi (Mobile internet use nearing 50% 2010). Vuoden 2011 helmikuussa Nokia ja Microsoft (2011) ilmoittivat yhteistyöstään, jonka tuloksena Nokia siirtyi käyttämään Windows Phone käyttöjärjestelmää puhelimissaan. Journalisti Dan Grabham (2010) kirjoittaa että jo ennen tätä, Nokian oli tarkoitus siirtyä Symbianista Linux –pohjaiseen MeeGo –käyttöjärjestelmään. Virallisen Nokian (2011a) Symbianin kehittäjille tarkoitetun verkkosivuston mukaan Nokia on kaikesta huolimatta sitoutunut Symbianin jatkuvaan innovaatioon. Opinnäytetyön tekijän mielestä on mielenkiintoista seurata Symbianin kohtaloa, sillä kasvavien markkinoiden kotimaisilla puhelinvalmistajilla, esimerkiksi Kiinassa, saattaisi spekulatiivisesti olla kiinnostusta Symbiania kohtaan.

BlackBerry OS on kanadalaisen Research In Motionin (RIM) älypuhelimissaan käyttämä käyttöjärjestelmä. RIM (2011a) on verkkosivustonsa mukaan valmistanut BlackBerry –tuotteita vuodesta 1999. Niihin kuuluu tänä päivänä PlayBook –sormitietokone, älypuhelin, yrityssovelluksia, sekä lisälaitteita. Dwivedi ym. (2010, 122-123) pitävät BlackBerry –älypuhelimia suosittuina valintoina yrityksille, koska ne salaavat käyttäjien lähettämät viestit automaattisesti ja niiden BlackBerry Enterprise Server (BES) hallintaohjelma antaa järjestelmänvalvojille hyvät mahdollisuudet valvoa puhelimia. BlackBerry älypuhelimien sovellukset ohjelmoidaan Dwivedin ym. (2010, 125) mukaan lähinnä Java –ohjelmointikielellä. RIM:in (2011b) BlackBerry App World verkossa olevasta sovelluskaupasta löytyy tällä hetkellä 30652 sovellusta.

Seuraava Kuva 2 hahmottaa vielä eri käyttöjärjestelmiä käyttävien älypuhelimien myynnin jakaantumista, sekä osoittaa kuinka kaikkien älypuhelimien myynti on kasvanut nopeasti. On tärkeää huomioida, ettei Symbiania käyttävien älypuhelimien määrän kasvu johdu pelkästään Nokian myynnistä, mutta iOS:ssää käyttävien iPhonejen määrän kasvu johtuu vain Applen myynnistä. Kuvan taulukon vuoden 2011 myynti perustuu spekulointiin.

OS	2009	2010	2011	2014
Symbian	80,876.3	107,662.4	141,278.6	264,351.8
Market Share (%)	46.9	40.1	34.2	30.2
Android	6,798.4	47,462.1	91,937.7	259,306.4
Market Share (%)	3.9	17.7	22.2	29.6
Research In Motion	34,346.8	46,922.9	62,198.2	102,579.5
Market Share (%)	19.9	17.5	15.0	11.7
iOS	24,889.8	41,461.8	70,740.0	130,393.0
Market Share (%)	14.4	15.4	17.1	14.9
Windows Phone	15,031.1	12,686.5	21,308.8	34,490.2
Market Share (%)	8.7	4.7	5.2	3.9
Other Operating Systems	1,.431.9	12,588.1	26,017.3	84,452.9
Market Share (%)	6.1	4.7	6.3	9.6
Total Market Sales	**172,374.3**	**268,783.7**	**413,480.5**	**875,573.8**

Kuva 2: Älypuhelimien myynti (tuhansissa) jaoteltuna niiden käyttämien käyttöjärjestelmien mukaan

Aikaisemmassa, Applen iOS -mobiilikäyttöjärjestelmää käsitellessä, kappaleessa mainittiin kuinka Apple toi ensimmäisenä markkinoille App Store –sovellusverkkokauppansa vuonna 2008. Älypuhelimille oli jo aikaisemmin olemassa Internetistä ladattavia sovelluksia, mutta ennen Applea kukaan ei ollut kerännyt kaikkia puhelimille tarkoitettuja sovelluksia samaan paikkaan. Muut valmistajat ilmeisesti huomasivat App Storen kiistämättömän suosion ja perustivat omat älypuhelimien sovelluksille tarkoitetut verkkokauppansa: Googlella on Android Market, Nokialla OVI Store ja BlackBerryllä App Store. CNCCS (Smartphone Malware 2011, 15) toteaa kaikkien muiden paitsi Googlen verkkokauppojen olevan samankaltaisia kuin Applen siinä mielessä, että niihin ladatut sovellukset tarkistetaan haittaohjelmien varalta ennen käyttäjille tarjoamista. Dwivedin ym. (2010, 22) kertovat että Googlen verkkokaupasta ladattujen sovellusten tietoturva perustuu siihen, että latauksen jälkeen ne kysyvät käyttäjän lupaa käyttää tiettyjä toimintoja varten. Google poistaa vasta jälkikäteen sille ilmoitetut haittaohjelmat verkkokaupastaan. CNCCS:n (Smartphone Malware 2011, 15) mukaan kaikkiin

sovellusverkkokauppoihin liittyy omat ongelmansa, eikä mikään niistä ole onnistunut pitämään haittaohjelmia loitolla.
Suoraan haittaohjelmiksi luokitellut sovellukset eivät suinkaan ole sovelluskauppojen ainoa ongelma. Lisää ongelmia käsitellään luvussa ”2.1 Aikaisemmat mobiilitietoturvaa koskevat metodit” tarkasteltaessa mobiilitietoturvan suojaukseen tarkoitettuja ohjeita ja vertailtaessa niitä nykyisiin tietoturvan vaarantaviin ongelmiin. Tässä opinnäytetyössä käytetyllä termillä ”sovellus” viitataan Internetissä ja yleensäkin lähes poikkeuksetta mobiililaitteiden ohjelmiin. Käyttöjärjestelmän päällä toimivien ja tietokoneen tekniseen toimivuuteen liittymättömien, eli normaalikäyttäjälle kaikkien, ohjelmien, ohjelmistojen ja sovellusten oikeaoppinen termi on sovellusohjelma (Atk-sanasto). Oli siis kyse sitten pöytätietokoneista tai älypuhelimista. Vertaa MOT-sanakirjan englanninkielisiin programme (am. program), ohjelma, ja application, sovellus. Huomioitavaa on, että esimerkiksi ohjelma ja ohjelmisto –termit tarkoittavat eri asioita, mutta kuten edellä mainittiin, peruskäyttäjälle ne ovat käytännössä sama asia.

Yrityksien tietoturvaa käsitellessä tietoturvaa koskeva käsitteistö laajenee ja monimutkaistuu. Seuraavassa kappaleessa käsitellään kertaukseksi tietoturvan peruskäsitteitä ja tämän jälkeen pyritään selittämään yrityksiin liittyvää sanastoa. Opinnäytetyön rajaamiseksi joudutaan jättämään paljon sanastoa ja selityksiä pois, joten asiasta kiinnostuneille suositellaan luettavaksi esimerkiksi Suomen Valtionhallinnon tietoturvallisuuden johtoryhmän, tästedes VAHTI, laatimia julkaisuja kuten Tietoturvallisuudella tuloksia (2007a).

Koska VAHTI (2007a, 13) määrittelee tietoturvan tarkoituksen ja tavoitteen selkeästi, on se seuraavassa suorana lainauksena: ” Tietoturvallisuudella tarkoitetaan tietojen ja palvelujen, järjestelmien ja tietoliikenteen suojaamista ja varmistamista niihin kohdistuvien riskien hallitsemiseksi sekä normaali- että poikkeusoloissa hallinnollisilla, teknisillä ja muilla toimenpiteillä. Tietoturvallisuuden tavoitteena on tietojen luottamuksellisuuden, eheyden ja käytettävyyden turvaaminen laitteisto- ja ohjelmistovikojen, luonnontapahtumien sekä tahallisten, tuottamuksellisten tai tapaturmaisten tekojen aiheuttamilta uhilta ja vahingoilta.” VAHTI (2008, 109) selittää vielä termejä: tiedon luottamuksellisuus tarkoittaa sitä että tietoon on pääsy vain niillä, joille se on tarkoitettu. Tiedon eheys sitä ettei tieto ole muuttunut luvattoman käsittelyn, siirron tai tallennuksen seurauksena. Tiedon käytettävyys sitä, että tieto on hyödynnettävissä silloin kun sitä tarvitaan. Seuraavaksi käytetään Tampereen Yliopiston (2009) laatimaa sanastoa selittämään seuraavat: tietoturvauhka, tietoturvariski, tietoturvan hallinnolliset, tekniset ja fyysiset suojaamismenetelmät.

Tietoturvauhalla tarkoitetaan uhkaa, kuten viruksia ja tietomurtoja, jotka vaarantavat jonkin edellä mainitun tiedon osa-alueen. Tietoturvariskillä viitataan todennäköisyyteen, jolla tietoturvauhka toteutuu. Tietoturvan suojaamismenetelmät, joiden tarkoitus on poistaa ja pienentää tietoturvariskejä, voidaan luokitella kolmeen kategoriaan: teknisiin, fyysisiin ja hallinnollisiin menetelmiin. Tekniset menetelmät tarkoittavat laitteistollisia ja ohjelmistollisia ratkaisuja, kuten palomuuria ja anti-virusohjelmia. Fyysisiä menetelmiä ovat esimerkiksi ovien lukitseminen ja paloturvallisuuden varmistaminen palo-ovilla ja sammuttimilla. Opinnäytetyön liitteinä olevat ohjeistot ja niiden esittely ovat eräänlaisia hallinnollisia menetelmiä. Suojaamismenetelmiä voidaan kutsua myös tietoturvamekanismeiksi. Tampereen yliopiston (2009) kokoama liitteenä neljä oleva käsitekartta ”Tietoturvamekanismien esittely”, esittelee lukijalle monta tärkeää tietoturvamekanismia ja näyttää eri mekanismien välisen vuorovaikutuksen. Käsitekartta voi vaikuttaa epäselvältä, mutta se on looginen. Käsitekartassa tietoturvan suojaamiseen tarkoitetuista teknisistä menetelmistä käytetään termiä informaatiolliset menetelmät.

Lähinnä yrityksille suunnattu VAHTI (2007a, 23-36) painottaa tietoturvan integroimista organisaation järjestelmiin, ja kertoo että tietoturvallisuuden pohjana olevan organisaation toimintaan liittyvien tietoriskien tunnistamisen ja arvioimisen. Näin voidaan tehdä päätökset siitä, mitä toimenpiteitä tulee toteuttaa. VAHTI:n (2007a, 23) mukaan riskejä hallittaessa on lähtökohdaksi otettava organisaation toiminnan kehittäminen, esimerkiksi johtaminen, osaaminen ja toimintatavat. Tämä tarkoittaa käytännössä, että organisaatiolla tulisi olla dokumentoituna erinäisiä politiikoita, strategioita ja suunnitelmia, tietyistä vastuualueista vastaavia henkilöitä, sekä aikeet toteuttaa laadittuja politiikoita, strategioita ja suunnitelmia. Edellä mainittujen tulee myös palvella organisaation liiketoimintaprosesseja mahdollisimman hyvin, eikä missään nimessä estää tai hankaloittaa liiketoimintaa.

Turvallisia prosesseja ylläpidettäessä ja kehitettäessä organisaation määrittelemillä tavoilla voidaan noudattaa VAHTI:ssa (2007a, 38) mainittua tietoturvastandardi ISO 27001 mukaista PDCA (Plan, Do, Check, Act) –prosessimallia. PDCA –prosessimallin vaiheet seuraavat toisiaan ympyrässä. Suunnitteluvaiheessa (Plan) prosessi käynnistetään suunnittelulla. Toteutusvaiheessa (Do) suunnitelmat realisoidaan. Tarkistusvaiheessa (Check) prosessin tilasta tuotetaan tietoa auditointien, valvonnan ja raporttien avulla. Viimeisessä vaiheessa, eli kehitysvaiheessa (Act), tarkistusvaiheessa saatuja tuloksia analysoidaan ja prosessia pyritään parantamaan tuloksien avulla, jotta prosessin lopputulos olisi entistä parempi. Tästä siirrytään takaisin suunnitteluvaiheeseen.

Sosiaalinen media on yksi nykyajan ohittamattomista termeistä. Termillä voidaan viitata useisiin asioihin, joista kaikki eivät ole yritysten kannalta samanarvoisia, kuten kolumnisti Perttu Tolvanen (2011) osoittaa. Tolvanen toteaa myös, etteivät avoimuus ja läpinäkyvyys lähtökohtaisesti tuota parempia tuloksia yritystoiminnan kannalta. Tietokone –lehden toimittaja Antti Tuurala (2011, 42-47) puolestaan kehottaa kaikkia yrityksiä ja yksityishenkilöitä ottamaan viimeistään nyt sosiaalisen median ohjat käsiinsä. Hyödyllisiksi sosiaalisen median, eli lyhennetysti somen, palveluiksi lehti luettelee yhteisöpalvelut, mashupit, erilaiset wikit, virtuaalimaailmat ja pikaviestinnän. Koska some on aiheena valtava, seuraavissa kappaleissa käydään lyhyesti läpi edellä mainitut termit.

Yhteisöpalveluja ovat esimerkiksi Facebook ja Google+. Niissä käyttäjä ensin rekisteröityy omalla tai keksityllä nimellä ja sen jälkeen siirtyy selaamaan muiden käyttäjien ja organisaatioiden tietoja ja tekemisiä. Käyttäjän vastuulle jää minkä verran hän haluaa itsestään kertoa muille ihmisille ja organisaatioille. Talouselämä (2011) paljastaa, että käyttäjät jotka haluavat pitää yksityisyydestään kiinni ja luulevat osaavansa käyttää sosiaalisen median palveluja, tekevät silti paljon virheitä ja altistavat tietonsa esimerkiksi kolmansien osapuolien saataviksi.

Mashupit ovat Tuuralan (2011, 42-47) mukaan Internetin eri palveluista yhdeksi kokonaisuudeksi rakennettuja palveluita. Tällaisia ovat esimerkiksi muokatut Spotifyn soittolistat ja karttapalveluita, joihin on lisätty kohdetietoa. Tuurala mainitsee mashupeiksi myös yrityksien intranetit, joissa saa muokattua esimerkiksi aloitussivun haluamansa näköiseksi. Wikipohjaisista palveluista kuuluisimmaksi Tuurala kertoo Wikipedian, josta on epäilyistä huolimatta muodostunut yksi Internetin käytetyimmistä tiedonhakukanavista. Alun perin tietokoneella pelaavien käyttämät virtuaalimaailmat ovat Tuuralan mukaan olleet osaltaan kasvattamassa sosiaalisen median suosiota ja kasvaneet pienen porukan virtuaaliyhteisöistä esimerkiksi opetus- ja työkäyttöön soveltuviksi työkaluiksi. Virtuaalimaailmoista Tuurala mainitsee Habbo-hotellin ja Second Worldin. Pikaviestimet tiivistyvät Tuuralan mukaan pitkälti Twitteriin, vaikkei se ole ainoa pikaviestinkanava. Yritykset voivat hyödyntää pikaviestiohjelmia hyvin asiakaspalvelussa, kuten Tuuralan mainitsema Polarin tytäryhtiö on tehnyt.

Somen palveluja käytetään kasvavassa määrin älypuhelimilla, kuten MarketingProfs:sin (2011) analysoima tutkimus vuoden 2011 huhtikuun ja toukokuun väliseltä ajalta paljastaa. Verkkosivuston mukaan 59 prosenttia älypuhelimien käyttäjistä vierailee puhelimellaan someksi luokitelluilla sivustoilla. Vertailun vuoksi mainittakoon, että 92 % käyttäjistä käyttää tekstiviestejä, 76 % sähköpostia ja 55 % paikannusta hyväksikäyttäviä sovelluksia.

Jos ajatellaan, että yrityksen älypuhelimien käyttäjistä 59 prosenttia käyttää puhelimellaan somea, tekee se Halti Oy:n tapauksessa noin kaksikymmentä henkeä, joka on noin kolmannes kaikista työntekijöistä. Kun sosiaalisen median palveluita käytetään älypuhelimilla, yhdistyy siihen molempien tietoturvauhkia. Tällaisia ovat esimerkiksi ladattavat haittasovellukset, jotka esittävät someen liittyviä sovelluksia, älypuhelimien näytöillä näkyvät liian lyhyet Internet-osoitteet ja työntekijän väärään paikkaan esittämät mielipiteet yrityksestä (Nemey, 2011). Asiaa eivät auta Bodkinin (2011) esittämät Ciscon huolet huijareiden siirtymisestä roskapostin lähettämisestä sosiaalisen median palveluihin.

Kaiken kaikkiaan Halti Oy:n mobiililaitteiden tietoturva on monista palasista koostuva verkosto, jonka turvaamiseksi liitteenä oleva ohjeisto on tarkoitettu. Ohjeisto koostuu lähinnä tietoturvan teknisten suojaamismenetelmien mekaanisesta käyttöönottamisesta, mutta myös tiedosta, jolla pyritään informoimaan mobiililaitteiden käyttäjiä. Uuden informaation on tarkoitus saada käyttäjät valppaiksi ja aktiivisesti miettimään valintoja mitä he mobiililaitteillaan tekevät. Ohjeiston luomisen ja asiakasyrityksessä esittelyn voidaan ajatella olevan mobiilitietoturvan kehittämisprosessin PDCA -mallin kaksi ensimmäistä vaihetta. Koska suojaamismenetelmiä on paljon, täytyy niistä poimia Halti Oy:lle sopivat. Kaikkien mahdollisten suojaamismenetelmien käyttöönottaminen ei välttämättä ole järkevää käyttäjän, eikä liiketoimintaprosessien suojaamisen näkökulmista. Seuraavassa luvussa kartoitetaan Halti Oy:n mobiilitietoturvan lähtötilannetta kehittämisprosessin alussa, ja siihen palataan luvussa ”2.1 Aikaisemmat mobiilitietoturvaa koskevat metodit”. Tietoriskien tunnistamiseen ja arvioimiseen palataan luvussa ”3. Uuden metodin kehittely”.

1.2 Halti Oy toimintaympäristönä

Tässä luvussa kerrotaan Halti osakeyhtiön liiketoiminnasta, siitä mikä on mobiilitietoturvan tilanne nyt ja miksi muutos on ajankohtainen. Seuraavassa esitettävät tiedot, laitteiston kuvausta lukuun ottamatta, ovat koostettu kaikille näkyviltä Halti Oy:n (2011) Internet – sivuilta. Halti Oy on vuonna 1976 perustettu suomalainen yritys, joka suunnittelee ja markkinoi ulkoiluvaatemallistoja, kenkiä, sekä retkeilyvarusteita kaikille vuodenajoille. Tuotteet suunnitellaan Suomessa ja tuotetaan Aasiassa, sekä erinäisissä muissa halpatuotannon maissa. Tärkeimmät tuotealueet, joita myydään Halti ja Raiski tuotemerkkien alla, ovat talviurheilu ja Outdoor Sports. Tuotteiden jälleenmyyjiä ovat urheilukaupat, tavaratalot ja marketit. Myyntipisteitä on yli 1400 yli viidessätoista eri maassa. Päämarkkina-alueet ovat Suomi ja Keski-Euroopan alppimaat. Halti Oy:n tuotteet jakautuvat kahteen tuotemerkkiin; Haltiin ja Raiskiin. Halti – tuotemerkin tuotteet kattavat laajan spektrin ulkoilulajeja: Alppi– ja freestylehiihdon, maastohiihdon, kiipeilyn, luontoliikunnan, juoksun, sauvakävelyn, golfin ja pyöräilyn.

Raiski – tuotemerkki kattaa koko perheen ulkoiluasut jokaiselle vuodenajalle. Raiskin mallisto tarjoaa myös D-mitoitetut tuotteet naisille. Vuonna 2011 valmistuu ensimmäiset Fischer -tuotemerkin ulkoiluvaatteet Halti Oy ja Fischer Sports GmbH yhteistyösopimuksen tuloksena. Kokonainen mallisto valmistuu vuonna 2012. Halti – tuotemerkki on suunnattu kaikenikäisille aktiiviulkoilijoille. Halti Oy panostaa tuotekehitykseen, jotta Halti – tuotteet sopivat vaativimmillekin lajiharrastajille. Raiski – tuotemerkki on suunnattu koko perheen ulkoiluun ja vapaa-aikaan ja se lähestyy kuluttajia ”vastinetta rahoille” – tyyppisellä hinnoittelumallilla.

Halti Oy:n pääkonttori sijaitsee Helsingin ja Vantaan rajalla Tuusulanväylän varrella osoitteessa Valimotie 5, Vantaa. Muita konttoreja yrityksellä on Munichissä, Salzburgissa and Shenzhenissä. Halti Oy:n lokakuussa 2011 avautunut Halti Store sijaitsee Helsingissä. Muita myyntipaikkoja ovat esimerkiksi Tanja Poutiainen Store joka sijaitsee Levillä ja Kalle Palander Store Rukalla. Halti Oy:llä on outletit Lauttasaaressa ja Herttoniemessä. Mainittavaa on myös, ettei Internet-osoitteessa http://www.haltistore.com/ oleva verkkokauppa ole Halti Oy:n omistuksessa, vaan sitä ylläpitää Partiovaruste Oy. Halti Oy:n osakkeista 51 prosenttia on yrityksen toimivan johdon omistuksessa ja 49 prosenttia pääomasijoitusyhtiö 3i:n omistuksessa. Halti Oy:n tietojen mukaan sillä oli vuonna 2010 60 työntekijää ja sen liikevaihdon suuruus oli noin 29 miljoonaa euroa. Halti Oy toimii läheisessä yhteistyössä mm. Ski Sport Finlandin kanssa, jonka avulla uusia tuotteita ja teknologioita voidaan testata käytännössä. Halti Oy:n muita yhteistyökumppaneita ovat mm. Audi, Fischer ja Plan.

Halti Oy:n edustajat eivät halunneet opinnäytetyöhön tarkkaa kuvausta laitteistosta tai Halti Oy:n toiminnasta tietoturvan suhteen. Tällä ei ole käytännössä merkitystä opinnäytetyön tekemisen tai tulkitsemisen kannalta, koska opinnäytetyön tekijä tietää nämä asiat ja välittää lukijalle kaiken tarvittavan tiedon. Esimerkiksi palvelimien nimillä ei ole mitään merkitystä opinnäytetyön kannalta. Halti Oy:n jokaisella työntekijällä on käytössä joko pöytätietokone tai kannettava tietokone Microsoftin Windows -käyttöjärjestelmällä. Tietokoneet päivitetään esiasennuksen yhteydessä ja automaattiset päivitykset otetaan käyttöön. Esiasennettavia ohjelmia ovat kaikille virustorjuntaohjelma ja Microsoft Office. Toiminnanohjausjärjestelmän liittymä, puhelinjärjestelmä, mobiililaitteen hallintaohjelma ja eri grafiikankäsittelyohjelmat asennetaan käyttäjän tarpeen mukaan. Jokaisella käyttäjällä on oma sähköpostiosoite, joka määräytyy käyttäjän nimen mukaan. Käyttäjätilejä hallinnoidaan keskitetysti Microsoft – palvelimelta Active Directoryn avulla. Haltin palvelinympäristö on virtualisoitu Haltin omille palvelimille, jotka ovat suojattu palomuurilla ja roskapostisuodattimella.

Halti tarjoaa mobiililaitetta tarvitseville työntekijöille mahdollisuuden matka- tai älypuhelimeen, joissa on normaalien ominaisuuksien lisäksi operaattorin rajoittamaton mobiililaajakaistayhteys. Jokainen laite täytyy hyväksyttää hankintalomakkeella ennen hankkimista. Operaattoriliittymiä Haltilla on n.45, joista suurin osa on älypuhelimille. Edellä mainittu Active Directory mahdollistaa monia hallintaominaisuuksia ActiveSync synkronointiteknologian avulla, koska Halti Oy:n sähköpostia tukeviin mobiililaitteisiin asennetaan lähes poikkeuksetta Mail For Exchange mobiilisähköpostisovellus. ”Pushmail”-tyyppisen sähköpostisovelluksen asetukset määritellään IT-osaston toimesta. Muita sovelluksia älypuhelimille ei asenneta etukäteen. Mobiililaitteissa on poikkeuksetta SymbianOS – mobiilikäyttöjärjestelmä, ellei työntekijä halua käyttää omaa laitettaan. Oman laitteen käyttö on siis sallittu. Yrityksen mobiililaitteet hankitaan poikkeuksetta yhdeltä ja samalta toimittajalta. Suurin osa puhelimien käyttäjistä käyttää Nokia Suite –ohjelmistoa, jonka avulla esimerkiksi puhelimessa olevista yhteystiedoista saadaan varmuuskopiot. Pieni osa yrityksen työntekijöistä käy työmatkoilla ulkomailla, kuten Euroopassa ja Aasiassa. Vantaan pääkonttorilla työntekijöillä on käytössään langaton verkko, josta on eristetty osuus Haltin vierailijoille. Lisäksi konttorilla on muutamia monitoimitulostimia. Haltin laitteistoa ylläpitää sen oma IT-osasto, johon kuuluu IT-manageri ja IT-spesialisti.

IT-spesialisti Joonas Tammiston mukaan Halti Oy:n mobiilitietoturva on toiminut tähän asti hyvin. Yksittäisiä ongelmia on hänen mukaansa ollut, mutta niitäkin hyvin harvoin. Laitteiden häviämisiä on ollut korkeintaan pari per vuosi, tiedostojen katoamisia tai laitteen häviämisiä toiset pari. Tammiston arvioiden mukaan suurimmat tietoturvauhat yrityksen mobiililaitteille ovat tällä hetkellä laitteiden varastaminen/katoaminen, sillä älypuhelimilla käytetään useita nettipalveluita ja sähköposteja, joiden salasanat ja tunnukset ovat puhelimen muistissa. Mobiililaitteen katoamistapauksessa sähköpostissa voi olla pahimmillaan, käyttäjän osastosta riippuen, muiden yritysten kanssa solmittuja sopimuksia, jotka ovat ehdottoman luottamuksellisia. Mobiililaitteissa säilytettävää tietoa ei ole luokiteltu.

Parannusehdotuksia mobiilitietoturvaan kysyttäessä, Tammisto listaa paremman Active Directory ActiveSync integraation ja puhelimien etähallinnan, etäpyyhinnän ja etälukituksen käyttöönottamisen. Vaikkei mobiililaitteiden kanssa siis ole ollutkaan pahempia ongelmia tähän saakka, monia hyviä tietoturvaan liittyviä ominaisuuksia ei ole ollenkaan käytössä. On tärkeää huomata, ettei laitteissa ole virustorjuntaohjelmaa, eikä laitteiston elinkaarta ole dokumentoitu. Mail For Exchangenin asennusta tai poistamista ei ole myöskään dokumentoitu. Lukijalle huomioksi, että vaikka aiemman luvun lopussa todettiin opinnäytetyön liitteenä olevan ohjeiston luomisen ja esittelemisen kiinnittyvän Halti Oy:n mobiilitietoturvan kehittämisprosessin PDCA -mallin suunnittelu- ja toteutusvaiheisiin, rakentuu opinnäytetyö myös aikaisemman PDCA –mallin ”pyörähdyksen” kehitysvaiheeseen. Tämä siis, vaikkei asiakasyritys käsittelisikään tietoturvaan liittyviä asioita PDCA –mallia hyväksikäyttäen.

Opinnäytetyön tekemisen kynnyskysymyksenä voidaan pitää sitä, ovatko Halti Oy:n tämän hetkiset toimet mobiilitietoturvan varmistamiseksi riittävät lähitulevaisuutta ajatellen? Haltilta kerättyä tietoa ja ulkopuolisia lähteitä tarkastellessa vastaus on ei. Tietoturvaa eivät uhkaa vain suorat varkaudet, vaan myös ohjeiston puuttuminen ja sitä kautta käyttäjien tietämättömyys. Jatkuvuuden kannalta on huono asia, ettei IT-osaston mobiililaitteiden esiasennusta, tai ylipäätään koko hankintaprosessia ole dokumentoitu. Lisäksi Halti Oy:n yhteyshenkilöt olivat halukkaita kehittämään mobiilitietoturvaa opinnäytetyöstä käydyissä keskusteluissa. Kaikkiin tietoturvaa uhkaaviin tekijöihin ei toisaalta kannata varautua, eikä yhdessä kehittämisprosessissa ottaa kantaa kaikkiin mahdollisiin asioihin, jo opinnäytetyön rajaamisen vuoksi. Miten mobiilitietoturvaa pitäisi kehittää? Tähän kysymykseen pyritään vastaamaan mahdollisimman täydentävästi luvussa ”3. Uuden metodin kehittely”. Seuraavassa luvussa esitellään ja vertaillaan eräitä opinnäytetyötä varten kerättyjä mobiilitietoturvaa koskevia ohjeita ja mietitään miten niitä voi parantaa, jotta uuden metodin kehittämiselle on hyvä pohja.

2 Yleiset toimintamallit

Tämä luvun tarkoituksena on käydä läpi aikaisempia mobiilitietoturvaa koskevia ohjeistoja ja vertailla niitä mobiililaitteiden nykytilaan. Suurin osa ohjeistosta koskee nimenomaan älypuhelimia, mutta niitä voidaan suurimassa määrin soveltaa myös normaaleihin matkapuhelimiin. Pääpaino liitteenä olevassa opinnäytetyön ohjeistossa ovat juuri älypuhelimet, mutta ohjeistoa voidaan soveltaa muihin matkapuhelimiin jättämällä tietyt kohdat pois. Myös sosiaalista mediaa koskevaa ohjeistoa käydään läpi asiakasyrityksen toiveesta. Luvussa tarkastellaan pitkälti VAHTI:n (2007b) antamaa ohjeistoa älypuhelimien tietoturvan turvaamiseksi, koska se oli ainut koko älypuhelimien elinkaaren kattava mikä löytyi tiedonhankinnan aikana. Ohjeisto on vuodelta 2007, joten sen sisältöä verrattiin tuoreempiin ohjeistoihin ja materiaaleihin, ja todettiin, ettei se ole pahasti vanhentunut. Muita tätä lukua varten poimittuja Mobiilitietoturvaa koskevia ohjeita ovat Tietokone –lehden Tero Lehdon (2011, 38-41) artikkelissa Mobiiliuhkat kuriin esiintyneet keinot älypuhelimen suojaamiseksi, Laurea AMK:n (2007a) intranet -verkkosivuilla olevat ohjeet älypuhelimien suojaamiseksi ja Viestintäviraston (2009) laatima Matkapuhelimen käyttäjän tietoturvaohje. Nämä tietyt ohjeistot ovat valittu, koska ne edustavat hyvin myös lukuisia muita tiedonhankinnassa löytyneitä ohjeistoja. Niissä mainitaan samoja suojaamismenetelmiä eri tavoilla muotoiltuna. Ohjeistot ovat myös luotettaviksi luettavista lähteistä. Halti Oy:llä ei ole omaa ohjeistoa.

Sosiaalinen media on paljon puhuttu aihe. On selvää, ettei kaikille maailman ihmisille kannata jakaa osoitetietojaan tai haukkua nykyistä työnantajaansa raskain sanakääntein. Mutta mitä sitten, jos osoitetiedot päätyvät puolivahingossa julkisiksi tai mitä laki sanoo työnantajan suoraan haukkumiseen? Vaikka luvussa 1.1. mainittu arvio siitä että yksi kolmasosa Halti Oy:n työntekijöistä käyttäisi somen palveluita työälypuhelimillaan, olisi liian korkea, on työntekijöiden ylipäänsä hyvä tietää someen liittyvistä riskeistä ja siitä mitä laki linjaa laittomiksi mielipiteiksi. Aihetta on käsiteltävä lyhyesti muutamaa esimerkkitapausta hyväksikäyttäen, jottei opinnäytetyö ota kantaa liian moneen asiaan. Sosiaalisen median ohjeet on poimittu Helsingin Sanomista Matti Tyynysniemen (2011) kirjoittamasta artikkelista, Laurea AMK:lta (2007b) ja VAHTI:sta (2010). Tyynysniemi (2011) ottaa kantaa lähinnä siihen mitä työntekijät saavat lain mukaan puhua esimerkiksi Facebookissa, kun toiset ohjeet antavat neuvoja tietoturvaan. Huomiota kannattaa kiinnittää siihen, että älypuhelimia ja sosiaalista mediaa koskevissa ohjeissa on monin paikoin samoja suojautumismenetelmiä.

2.1 Aikaisemmat mobiilitietoturvaa koskevat metodit

Luvussa ”1.2 Halti Oy toimintaympäristönä” käsiteltiin jo Halti Oy:n tähän asti hyvin toimineita toimintatapoja mobiilitietoturvan suhteen. Lisättävänä on, että työntekijät ovat osanneet toimia oikein laitteiden katoamistapauksissa, vaikkei niistä ohjeita ole jaettukaan. Lisäksi harvalla työntekijällä on esimerkiksi muiden organisaatioiden kanssa laadittuja sopimuksia sähköpostissaan. Kaiken huomioon ottaen Halti Oy:n toimintatavat ovat olleet käytännössä valideja ja kaiketi myös realistisia, koska aikaisemmin älypuhelimille suuntautuneita uhkia on ollut vähemmän, eikä mitään matkapuhelimen menettämistä vakavampaa ole sattunut. Yksi syy siihen ettei mitään vakavampaa ole aiemmin sattunut voidaan katsoa olevan yksinkertaisesti se, ettei Halti Oy:llä ole aikaisempina vuosina ollut yhtä tehokkaita älypuhelimia kuin mitä sillä on nyt. Tulevaisuutta varten täytyy kuitenkin tarkastella mitä eri julkaisuissa neuvotaan yrityksen mobiilitietoturvan suojaamiseksi.

Ensimmäiset ohjeet ovat Tietokone –lehdestä, jonka artikkelissa haastatellaan mm. tietoturvayhtiö Nixun kehittäjäyksikön johtajaa ja Elisan yritysasiakkaiden yhteyspalveluiden johtajaa. Toiset ohjeet ovat ammattikorkeakoulu Laurean näkökulmasta lehtoreille tarkoitetut. Kolmannet ohjeet ovat Viestintävirastolta ja niiden käyttämiseen ohjaa mm. CERT-FI tietoturvaviranomainen. Viimeiseksi käydään läpi VAHTI:n antamaa älypuhelimien ohjeistoa, joka sisältää koko älypuhelimen elinkaaren ja on kaikista ohjeista laajin, ja listataan typistetysti sen neuvomat hyvät käytännöt. On huomioitavaa, että opinnäytetyössä ohjeisto termiä käytetään kuvaamaan yhteen paikkaan kerättyjä ohjeita, vaikka ohjeista käytetään myös monikkomuotoa.

Tämän luvun olisi voinut periaatteessa toteuttaa kysellen eri yrityksiltä niiden mobiilitietoturvaohjeistoja, mutta silloin opinnäytetyössä olisi pitänyt keskittyä myös oikeanlaisen kyselyn tuottamiseen ja luottaa siihen, että yritykset vastaisivat kyselyihin. Kyselyssä olisi voitu myös kysyä eri yritysten vastoinkäymisiä mobiilitietoturvassa. Tässä opinnäytetyössä se olisi kuitenkin ollut jokseenkin turhaa, sillä luvussa ”1.2 Halti Oy toimintaympäristön” käytiin Halti Oy:n vastoinkäymisiä läpi ja tässä luvussa käydään globaaleita vastoinkäymisiä läpi. Opinnäytetyön tekijä ei myöskään usko, että ohjeistot olisivat poikenneet seuraavista, sillä ohjeistoja kerätessä on pyritty hankkimaan mahdollisimman hyvät ohjeet.

Tietokone –lehden Tero Lehdon (2011, 38-41) kirjoittama artikkeli on kaikista ohjeisto – lähteistä tuorein. Siinä annetaan suoraan joitakin ohjeita ja keskustellaan myös yrityksien näkökulmista. Lehdon suoraan listaamat toimet älypuhelimen turvaamiseksi:

- Käytä pin-koodia, jota ei voi helposti arvata
- Hyödynnä lukituskoodia, kun laitteessa on arvokkaita tietoja
- Katso, tukeeko laite lukitusta tai tyhjennystä, jos pääsykoodi annetaan väärin
- Asenna päivitykset ja haavoittuvuuksien korjaukset heti
- Älä avaa epäilyttäviä viestejä tai liitetiedostoja myöskään mobiililaitteella
- Käytä tiedostojen salausta
- Älä tallenna mobiililaitteeseen luottokorttinumeroita tai muita salaisia tietoja
- Varaudu ennalta laitteen katoamiseen tai varastamiseen, jotta tiedät miten toimia.

Muita artikkelista poimittuja ohjeita yrityksille ovat suomalaisen teleoperaattori Elisan ja TeliaSoneran sekä tietoturvayhtiö Nixun suositukset tietoturvaohjelman asentamisesta älypuhelimiin. Ohjelmallisen virustorjunnan ja palomuurin saa teleoperaattoreilta heidän mukaansa halvimmillaan 2,5 eurolla kuukaudessa. Nixun kehittäjäyksikön johtaja Lauri Vuornoksen mukaan yrityksien on arvioita miten suuri vahinko tapahtuu, jos tiedot pääsevät vuotamaan ulkopuolisille, ja mille kaikille käyttäjäryhmille on tarpeen sallia pääsy sähköposteihin mobiililaitteella. Vuornos neuvoo, että ennen laitteiden käyttöönottoa voidaan tiedot luokitella sen mukaan, mitä ylipäätään saa viedä mobiililaitteisiin. Artikkelissa mainitaan myös Microsoft Exchangen käytön yhteisten sääntöjen asettaminen. Elisan Okkonen ja Nixun Vuornos ovat yhtä mieltä siitä, että parhaat ominaisuudet etähallintaan ovat tällä hetkellä Symbian -puhelimissa ja erityisesti Nokian E-sarjan malleissa. Syksyllä julkaistu Mango-päivitys tuo uusia ominaisuuksia yrityskäyttöön, mutta esimerkiksi tiedostojen salausta ei ole vielä mukana. Elisan Okkonen toteaa vielä, että yrityksissä voi olla perusteltua kieltää laitehallinnan kautta omien ohjelmien asentaminen tai ainakin rajata sallitut ohjelmat.

Artikkelin lopussa mainitaan, että kaikkien käyttäjien on ensiarvoisen tärkeätä tietää mitä laitteen kadotessa tulee tehdä.
Laurea-ammattikorkeakoulu (2007a) neuvoo seuraavat keinot matkapuhelimien suojaamiseksi ja pyrkii selvästi saamaan käyttäjät tutustumaan paremmin matkapuhelimiinsa:

- lue matkapuhelimen käyttöohje
- aseta SIM-kortin PIN-koodiksi vähintään 5 numeroa
- aseta puhelimen suoja/lukkokoodiksi vähintään 5 numeroa
- aseta puhelimen automaattisen lukituksen viiveeksi vähintään 15 minuuttia
- muista suojautuminen haittaohjelmilta
- mieti mitä tallennat puhelimeesi
- muista, että soittopyyntö tai tekstiviesti voi olla huijausyritys
- ole huolellinen bluetoothin ja langattomien tekniikoiden kanssa
- huomioi kotimaan ulkopuolella tapahtuvan käytön mahdolliset operaattorikohtaiset rajoitukset ja kustannukset
- tiedä miten toimit katomistilanteessa!

Samalla sivulla neuvotaan myös miten tulee toimia mobiililaitteen katoamistilanteessa. SIM-kortin katoamistapauksessa sivut käskevät ottamaan yhteyden operaattorin asiakaspalveluun, jonka yhteystiedot on mainittu. Mikäli käyttäjä on käyttänyt Laurean sähköpostia, tulee sen salasana välittömästi muuttaa tietyssä verkko-osoitteessa. Tämän jälkeen käyttäjän tulee ilmoittaa oman paikallisyksikkönsä yrityspäätevastaavalle ja IT-palveluiden helpdeskiin.

Viestintäviraston (2009) Matkapuhelimen käyttäjän tietoturvaohje ei sisällä erityisiä neuvoja yrityksille, mutta kertoo lyhyesti ja selvästi miltä suojautumismenetelmät suojaavat. Viestintävirasto (2009, 2) tiivistää matkapuhelimien tietoturvan kolmeen askeleeseen:

- Älä paina matkapuhelimen Kyllä/Yes-näppäintä, ellet ole varma seurauksista.
- Tuhoa tuntemattomalta lähettäjältä tullut MMS-viesti avaamatta sitä.
- Jos sinulle tuntematon laite yrittää ottaa Bluetooth-yhteyttä, liiku muutama kymmenen metriä paikaltasi: yhteys katkeaa automaattisesti.

Pidemmän listan kohdat, joissa myös syvennetään aiheita, ovat seuraavat, ilman syventäviä neuvoja:

- Lue puhelimesi käyttöohjeesta erityisen huolellisesti seuraavat kohdat:..
- Huolehdi, että matkapuhelimessasi on päällä PIN-kysely
- Käytä operaattorien tarjoamia esto- ja rajoituspalveluita
- Muista, että matkapuhelin sisältää paljon tietoa käyttäjästään

- Huolehdi matkapuhelimestasi kuin luottokortistasi. Jos annat tai lainaat puhelimesi toiselle, muista että:..
- Muista, että sinulle voidaan soittaa tai lähettää viestejä huijaustarkoituksessa
- Ole huolellinen Bluetoothin ja muiden langattomien tekniikoiden käytössä
- Käytä harkintaa ohjelmia asentaessasi

Ohjeissa neuvotaan vielä ottamaan teknisissä ongelmissa yhteys matkapuhelimen jälleenmyyjään tai huoltopisteeseen. Jos käyttäjä epäilee joutuneensa tietoturvaloukkauksen kohteeksi, häntä neuvotaan ottamaan yhteys operaattoriin, matkapuhelimen huoltoliikkeeseen, viestintävirastossa toimivan CERT-FI:n tai muun mobiilitietoturva-asiantuntijan puoleen.

VAHTI (2007b) antaa kaikista kattavimman ohjeiston, koska se käsittelee laitteiston koko elinkaarta ja antaa selkeät syyt suojaamismenetelmien käyttöönottamiselle. Ohjeisto on alun perin tarkoitettu organisaatioiden johdolle ja kaikille niille henkilöille, jotka vastaavat organisaation älypuhelimiin liittyvistä toiminnoista. Seuraavassa on ohjeistossa esiintynyt tiivistetty lista älypuhelimien käytön turvallisuudessa huomioon otettavista seikoista. Listasta on typistetty pois syventävät neuvot ja syyt suojaamismenetelmien käyttöönottamiselle:

a) SIM-kortti ja liittymä
- pin-suojauksen käyttöönotto
- puhelimen automaattilukitus 5 – 10 minuutin aikaviiveellä
- liittymään ei kannata aktivoida sellaisia palveluita, joita sillä ei ole tarkoitus käyttää (esimerkiksi MMS-palvelu, multimediaviestien käyttöön ei ole välttämättä kaikilla käyttäjillä tarvetta)
- data-yhteyksien osalta kannattaa pyrkiä yksittäisten data-pakettien sijaan hankkimaan isompi datapooli, joka mahdollistaa vapaammin datayhteyksien hyödyntämisen.

b) Haittaohjelmien torjunta
- automaattisesti itsensä päivittävä haittaohjelmien torjuntaohjelma, jossa on lisäksi mahdollisuus palomuuritoimintoihin
- älypuhelimen salakirjoitusohjelmiston käyttö on suositeltavaa

c) Tietoliikenneyhteydet
- Älypuhelimen bluetooth-yhteydet pitää poistaa käytöstä, jos käyttäjä ei käytä bluetooth-laitteita. Jos yhteydelle on tarvetta, pitää asetukset saattaa siihen tilaan, että bluetooth-yhteydet eivät mainosta laitetta muille bluetooth-laitteille eli tila on piilotettu.

d) Etähallinta

- etähallinta on keskeinen ohjelma tietoturvallisuuden toteuttamisessa älypuhelinympäristössä, koska sillä voidaan rajoittaa useimpia älypuhelimen käyttöön liittyviä toimintoja sekä vastata älypuhelimen vakiointiin ja varmistamiseen liittyvistä toiminnoista.
- käyttäjiä tulee tiedottaa puhelinten etähallintamahdollisuudesta
- käyttäjää tulee tarpeen mukaan tiedottaa etähallinnalla tehtävistä toimenpiteistä etukäteen

VAHTI (2007b, 26) ottaa epäsuorasti kantaa sovelluskauppoihin kehottaessaan kieltämään käyttäjiltä sovellusten asentamisen käytettävyys-, tietoturva- ja ohjelmistolisenssiteknisistä syistä. Ohjeisto on ainoa, jossa käsitellään sähköpostin ja kalenterin synkronointia ja varoitetaan käyttäjiä ulkomailla tulevista ylimääräisistä datansiirtomaksuista. VAHTI (2007b, 30) mainitsee myös, että älypuhelinympäristön tehokas hyödyntäminen edellyttää parin tunnin mittaista käyttökoulutusta. Tähän koulutukseen oleellisesti liittyvässä käyttöohjeessa tulee olla tarkasti ohjeistettuna elinkaarenhallinnan kannalta loppukäyttäjälle kriittiset osa-alueet. Esiasennuksesta ja vakioinnista VAHTI (2007b, 27) toteaa, että pienissä yrityksissä saatetaan saavuttaa parhaat tulokset käyttäjän asentaessa puhelimensa itse hyvien ohjeiden avulla, mutta suuremmissa yrityksissä esiasennuksen ja vakioinnin merkitys korostuu.

Kaiken kaikkiaan ohjeistot antavat selkeän kuvan siitä miten mobiilitietoturva hoidetaan hyvin. Moniin asioihin on varauduttava, koska älypuhelimet muistuttavat enemmän tietokoneita, kuin perinteisiä matkapuhelimia. Nykyajan ”perinteiset matkapuhelimetkin” alkavat muistuttaa enemmän ja enemmän tietokoneita. Langaton tiedonsiirtokaan ei ole ongelmatonta. Kun kaikkia ohjeistoja tarkastelee samanaikaisesti, voi ne opinnäytetyön tekijän mielestä luokitella valideiksi ja realistisiksi. Peruskäyttäjille niistä kaikista löytyy olennaisia keinoja tietoturvauhkia vastaan varautumiseen, varsinkin kun mobiililaitteen katoaminen on esimerkiksi Halti Oy:n tapauksessa todennäköisin ja vakavin uhka. Tämä ei tarkoita ettei niitä voi parantaa. Seuraavassa luvussa käsitellään parannusideoita tämän luvun ohjeisiin. Seuraavat kappaleet esittelevät sosiaalisen median palveluiden käyttäjille tarkoitettuja ohjeita. Ohjeet on pyritty valitsemaan niin, että niistä voidaan koostaa Halti Oy:n työntekijöille hyvä ja luotettava sosiaalista mediaa koskeva ohjeisto. Periaatteessa tähän riittäisi vain VAHTI (2010), mutta vertailun vuoksi käsitellään myös muita ohjeita. Näin voidaan kerätä uutta ohjeistoa varten benchmarkin –tyyppisesti usein esiintyvät käytänteet. Halti Oy:llä ei ole sosiaalista mediaa koskevaa ohjeistoa ennestään.

Huomioitavaa on, ettei opinnäytetyön tarkoitus ole luoda Halti Oy:lle politiikkaa ja valmista koulutusta koskien sosiaalista mediaa. Opinnäytetyön tarkoitus on enemmänkin tiedottaa Halti Oy:n työntekijöitä ja antaa mahdollisesti eväät ja suuntaviivat virallisen politiikan luomiselle. Liitteenä olevien ohjeistojen luomiseen on kuitenkin suhtauduttu virallisesti VAHTI:n (2007; 2007b; 2010) antamia ohjeita mukaillen.

Helsingin Sanomien artikkelissa Tyynysniemi (2011) summaa seuraavat ohjeet yrityksien työntekijöille siitä mitä he saavat ja eivät saa sanoa sosiaalisen median palveluissa:

Ei ainakaan näin:

- Pomon julkinen haukkuminen
- Liikesalaisuuksien paljastaminen
- Työnantajaa vahingoittavat puheet

Vähintään rajatapauksia:

- Omalle työnantajalle kielteisten tosiasioiden kertominen
- Julkisesti esitetyt voimakkaat mielipiteet
- Työhön tai työnantajaan liittyvien asioiden kommentointi julkisuudessa

Pitäisi voida puhua:

- Oman työsuhteen ehdot, kuten palkka
- Arkiset asiat, kuten lomat ja vapaat
- Luottamusmiehille ja viranomaisille voi aina puhua

Artikkelissa SAK:n lakimies Anu-Tuija Lehto kommentoi työntekijän oikeuksia työnantajasta puhumiseen raskaasti: ”Oikeuskäytännöstä voi tehdä sen johtopäätöksen, että olkaa hiljaa”. Asianajaja Anu Kaisko on hieman samaa mieltä ja muistuttaa että epäselvissä tilanteissa työntekijän on parasta laittaa ”suu suppuun”.

Laurea AMK antaa eräässä toisessa lähteessä kokonaisvaltaiset ohjeet sosiaalisen median palveluiden käyttämiseen, mutta seuraavassa on Laurea AMK:n (2007b) tietoturvaan ja tekijänoikeuksiin liittyvät ”perusvinkit”:

- Huolehdi, että sinulla on voimassaoleva haittaohjelmien suojaus tietokoneessa ja kännykässä.
- Valitse yksilöllinen ja monimutkainen salasana, joka ei ole ulkopuolisten arvattavissa.
- Älä käytä Laurean tietoverkon käyttäjätunnusta tai salasanaa sosiaalisen median välineissä.

- Älä hyväksy verkostoon tuntemattomia henkilöitä.
- Älä avaa epäilyttäviä linkkejä tai viestejä.
- Huolehdi omasta ja muiden yksityisyyden suojasta
- Lue käyttämäsi palvelun käyttöehdot

Ohjeissa käsketään työntekijää noudattamaan Laurean käyttösääntöjä työntekijän ollessa Laurean verkossa tai käyttäessään Laurean työvälineitä. Ohjeissa kerrotaan myös, että Laurea voi joutua tietoturvasyistä rajoittamaan tai kieltämään joitain somen palveluita ja kerrotaan miksi työntekijän tulee lukea käyttämänsä palvelun käyttöehdot. Työntekijää kehotetaan hakemaan lisätietoa VAHTI dokumentista ”Sosiaalisen median tietoturvaohje” (2010) ja lukemaan intranetistä Laurean sosiaalisen median ohjeet.

Kuten VAHTI:n (2007b) älypuhelimien ohjeisto, myös VAHTI:n (2010) sosiaalista mediaa koskeva ohjeisto on kaikista kattavin. VAHTI (2010) kattaa sosiaaliseen mediaan liittyvät riskit ja yrityksen sosiaalisen median ohjeiston käyttöönotossa huomioitavat seikat. Seuraavassa on listattuna VAHTI:n (2010, 28-29) ohjeet siihen, mihin yrityksen sosiaalisen median ohjeistuksessa ja koulutuksessa tulee kiinnittää huomiota:

- Verkkoidentiteettien käyttäminen
- Mitä organisaatioon toimintaan liittyvää saa kertoa ja mitä ei?
- Mitkä ovat yleiset käyttäytymissäännöt?
- Suositukset liittyen palveluiden yksityisyysasetuksiin (privacy settings)
- Käyttöehtojen lukemisen tärkeys
- Salasanaturvallisuus
- Hyvän salasanan luominen
- Eri salasanojen käyttö eri palveluissa
- Suositus etsiä hakukoneilla omalla nimellä mahdollisten identiteettivarkauksien löytämiseksi
- Kehotus huolellisuuteen verkostoiduttaessa ja kontaktien hyväksymisessä
- Kehotus varomaan haittaohjelmia
- Kehotus olemaan varuillaan kun napsuttelee lyhennettyjä url-osoitteita
- Tiedota kalasteluviestien yleispiirteistä ja kehota olla vastaamatta niihin
- Kerro kolmannen osapuolen sovelluksista ja niiden riskeistä, kehotus käyttämään harkintaa

Seuraavassa ohjeet siihen, mihin työntekijöiden kannattaa kiinnittää huomiota yksityisyytensä suojaamiseksi:

1. Identiteettivarkauksien hankaloittamiseksi kannattaa tutustua tarkkaan käytettävän palvelun tarjoamiin yksityisyyden suoja-asetuksiin ja useimmissa tapauksissa säätää ne oletusasetuksia tiukemmiksi
2. Julkiset sosiaalisen median palvelut sisältävät erilaisia mekanismeja unohdetun salasanan palauttamiseen. Tulee miettiä tarkkaan, millaisia keinoja sallii salasanan palauttamiseksi. Esimerkiksi salasanan palauttamisen mahdollistavassa menetelmässä pitää välttää kysymyksiä tyyliin ”Mikä on lemmikkisi nimi?”, koska vastaus saattaa löytyä suoraan henkilön palvelussa kertomista tiedoista. Suositeltavampaa on käyttää salasanan palauttamista lähettämällä sen muuttamisen mahdollistava linkki käyttäjän oletussähköpostiosoitteeseen.
3. Tulee miettiä, kannattaako esim. omaa syntymäaikaa, -paikkaa ja muita osoitetietoja kertoa, koska todennäköisesti ne henkilöt, jotka kyseisiä tietoja tarvitsevat, tietävät ne muutenkin
4. Sosiaalisen median palveluihin kerrottavaa tietoa kannattaa harkita kuten suunniteltaessa työaseman vakiointia ja ohjelmistokannan minimointia (eli sallia työasemassa käytettäväksi vain ne sovellukset joita tarvitaan); sosiaalisen median palvelussa kerrotaan vain se, mikä on välttämätöntä palvelun toiminnan kannalta
5. Valokuvia julkaistaessa kannattaa kiinnittää huomio kuviin mahdollisesti liitettyihin paikkatietoihin.

VAHTI (2010, 36-37) listaa vielä kymmenen ohjetta käyttäjälle, mutta ne ovat lähinnä koosteet kahdesta aiemmasta listasta. VAHTI:n (2010) ohjeet ovat kaiken kattavat ja huomioitavia kohtia ovat esimerkiksi varoitus lyhyistä URL:eista ja kuvien paikkatiedoista, joita ei huomioitu VAHTI:n (2007b) älypuhelimia koskevassa ohjeistossa. Kaiken kaikkiaan sosiaalista mediaa koskevat ohjeet ovat monelta kohdin samankaltaisia älypuhelimien tietoturvaohjeistojen kanssa. Molemmissa korostetaan esimerkiksi salasanojen tärkeyttä, haittaohjelmien varomista ja tietojen hallitsemisen tärkeyttä. Edellä mainittuja sosiaalisen median ohjeita voidaan pitää realistisina ja valideina, kun niitä vertaillaan toisiinsa ja muihin ohjeisiin. Niissä ei tosin käsitellä sosiaalisen median tulevaisuutta mitenkään, kuten käyttäjälle entistä enemmän monimutkaistuvampaa Facebookkia. Moni Facebookin käyttäjä ei luultavasti ymmärrä miksi Facebookin voi nykyään luokitella ”badwareksi”, josta eri Internet-selaimien tuottajien tulisi varoittaa Dashin (2011) mukaan. VAHTI (2010) ja Laurea AMK (2007b) varoittavat sentään tekijänoikeuksista, jotka käyttäjä julkaistessaan tuottamaansa materiaalia eri sosiaalisen median palveluissa voi menettää somen palveluja pyörittäville yrityksille.

Tomminen (2011) paljastaa yhden mobiililaitteiden heikkouksista kesän 2011 digitaalisten varmenteiden murtoa puidessaan. Kaikki suuret selainvalmistajat estivät melko nopeasti kaikki DigiNotar –yrityksen varmenteita käyttävät suojatut yhteydet varmenteiden vaarantumisesta kuultuaan. Ainoa minkä ne jättivät päivittämättä, olivat älypuhelimien selaimet, koska mobiilijärjestelmien valmistajat eivät halunneet vaarantaa matkapuhelinoperaattoreiden palveluita. Älypuhelinten päivittämistä ei ollut tehty vielä Tommisen (2011) kirjottaessa artikkelia syyskuussa. Tämä on harmillinen ongelma, sillä käyttäjät eivät pysty tekemään asialle muuta kuin olemaan valppaita, eikä sekään välttämättä auta.

Tässä luvussa mainittuihin ohjeistoihin liittyviä vastoinkäymisiä ei voi käytännössä käydä läpi, koska ohjeistoihin liittyviä tilastoja ei ole. Jos ohjeistoja on noudatettu, ovat ne mitä varmimmin toimineet. Mobiilitietoturva on siis saatu siirrettyä tiettyjä askelia seuraamalla alkutilasta lopputilaan, eli tietoturvalliseen mobiililaitteeseen. Esimerkiksi DataLossDB (Data Loss Statistics 2011) kertoo, ettei henkilötietoja ole globaalilla mittakaavalla vuotanut älypuhelimien kautta vuodesta 2002 tähän päivään lähes ollenkaan. Toisaalta viime päivinä on käsitelty paljon News of the World –lehden puhelinsalakuuntelu tapausta, jonka seurauksena Helsingin Sanomat (Salakuuntelussa ryvettynyt News of the World lopetetaan 2011) uutisoi että koko News of the World –lehti lopetettiin.

2.2 Parannusideat metodeja varten

Kaikki mobiililaitteiden tietoturvaa koskevat ohjeistot ovat selkeitä, mutta vain VAHTI:n ja Viestintäviraston ohjeistot selittävät käyttäjälle miksi suojaamismenetelmät tulee toteuttaa. Tämä on Talouselämän (2011) ja Karjalaisen ja Puhakaisen (2011) mukaan tärkeätä, jotta tietoturvakoulutus olisi tehokkaampaa. Talouselämä (2011) toteaa artikkelissaan, että tutkimustulosten perusteella voidaan todeta, ettei pelkkä tietoturvakoulutus riitä. Tietoturvakoulutusohjeistoihin tulee sisällyttää tietoja, mitä ihmisille on tapahtunut, kun he eivät ole olleet tarkkoja yksityisyytensä suojaamisessa. Samojen tutkimustulosten mukaan ruudulla näkyvä varoitus tai yksityisyyden suojaohje ei näytä tuovan mitään eroa. Käyttäjä, joka oli lukenut ohjeet, ei tiennyt yksityisyyden suojasta enempää, ei käyttäytynyt erilailla eikä ollut huolestuneempi käyttöjärjestelmistä kuin käyttäjä, joka ei ollut lukenut ohjetta.

Karjalaisen ja Puhakaisen (2011) esittämän yli 50 maassa tehdyn selvitystyön mukaan ”kaikkea kaikille” –tietoturvakoulutus ei toimi, koska syyt laiminlyönteihin ovat erilaisia: salasanaohjeita jätetään noudattamatta eri syistä kuin Internetin käyttöön liittyviä. Karjalainen ja Puhakainen (2011) kertovat tietoturvakoulutuksen olevan tehokasta vain, jos käyttäjä ymmärtää miksi tietyt toimintatavat ovat turvattomia. Tehokas koulutus liittyy myös suoraan kunkin koulutettavan työtehtäviin. Työntekijöille on selvitettävä, minkälaista

turvattavaa tietoa heidän työtehtäviinsä liittyy, ja mitä tapahtuu jos sitä ei suojata kunnolla. Karjalaisen ja Puhakaisen (2011) mukaan on tärkeää myös tuoda esiin se että tietoturvauhkat koskevat kaikkia työntekijöitä, ja että yrityksen johto ja esimiehet ovat sitoutuneet noudattamaan tietoturvaohjeita. Karjalainen ja Puhakainen (2011) summaavat suostuttelun olevan rangaistuksia ja tiukempaa valvontaa tehokkaampi koulutuskeino ja monen nykyisen tietoturvaohjeiston olevan liian ylimalkainen toimiakseen. VAHTI (2007b) ja Viestintäviraston (2009) ohje ovat siis tässä suhteessa parhaimpia, koska ne kertovat mitä uhkia suojaamismenetelmiin liittyy. Viestintävirasto (2009) kertoo tämän ehkä selkeimmin.

Ainoa ohjeisto, joka mainitsi älypuhelimiin liittyvänä uhkana gps-paikannusteknologian, oli VAHTI (2007b), eikä sekään käsitellyt paikannusta muuten, kuin listaamalla sen tulevaisuuden uhkaksi. Kauppalehti (2011) ja Turun Sanomat (2011) käsittelivät peräkkäisinä päivinä Tietoturva ry:n tietoturva-asiantuntija Pete Niemisen haastattelua. Nieminen toteaa haastattelussa rikollisten jo ajoittain seuraavan esimerkiksi TripIt –palvelua, jossa käyttäjät voivat jakaa matkasuunnitelmiaan. Palvelua käyttävät Niemisen mukaan myös virka- ja liikemiehet. Turun Sanomat (2011) kertoo myös Dealium –mainospalvelusta, joka paikantaa puhelimen ja etsii lähellä olevat tarjoukset tekoälyn kerätessä samalla tietoa tarjousvalinnoista. Nieminen toteaa, etteivät Dealiumin kaltaiset yritykset voi toimia pelkällä paikannusmarkkinoinnilla. Esimerkiksi Foursquaren toiminta perustuu siihen, että paikannustiedot linkitetään Facebookiin. Monet vastaavista paikannusyrityksistä, joko jakavat tai myyvät paikkatietoja eteenpäin.

Masalin (2011) osoittaa, etteivät pelkästään erilliset sovellukset talleta paikkatietoja luvatta: esimerkiksi iPhonet keräsivät paikannustietoa käyttäjän tietämättä ennen tänä vuonna tullutta ohjelmistopäivitystä. Nykyisin Apple vakuuttaa, että kerää tätä tietoa anonyymisti. iPhonen kameran ominaisuuksiin myös kuuluu se, että se liittää otettuihin kuviin sen hetkiset paikannustiedot. Kaikki paikannuspalveluihin liittyvät uhkat eivät tule vain yrityksien tai valtioiden suunnasta. Frilander (2011) kertoo, että kolmasosa ihmisistä vakoilisi puolisonsa matkapuhelimen sijaintia, jos se olisi mahdollista. Vanhemmista taas yli puolet vakoilisi lastensa matkapuhelimien sijaintia. Frilander (2011) tietää kertoa, että Suomessa paikannus vaatii periaatteessa käyttäjän luvan ja ilman suostumusta paikannusta käytetään vain hätätapauksissa poliisin tai pelastusviranomaisten toimesta. Frilander (2011) osoittaa myös muunlaisia tietoturvaloukkauksia: 41 prosenttia naisista sanoi katsoneensa puolisonsa sähköposteja tai puhelutietoja, 32 prosenttia miehistä on tehnyt samoin, ja 40 prosenttia vanhemmista on tutkinut lastensa viestejä. Nuorilla tilastot ovat vielä korkeammat: puolet alle 25-vuotiaista naisista ja 38 prosenttia samanikäisistä miehistä on kurkistanut seurustelukumppaneidensa puhelimiin. Opinnäytetyön tekijä katsoo, että Halti Oy:n käyttäjille on mainittava paikannuksen vaaroista.

VAHTI:n (2010) ja Laurea AMK:n (2007b) sosiaalisen median ohjeet eivät ota esimerkiksi huomioon aivan viime päivinä Facebookin käyttöönsä ottamia uusia ominaisuuksia. Dash (2011) käy läpi näitä ominaisuuksia ja toteaa niiden olevan vaarallisia Facebookin käyttäjille. Opinnäytetyön tekijän mielestä läpikäydyistä muutoksista seuraavat luultavasti kiinnostavat yrityksiä: käyttäjät eivät voi enää tuoda omaa sisältöään Facebookkiin RSS:n avulla; Facebook varoittaa käyttäjiä Internet-sivuista, jotka ovat turvallisia; ja Facebook alkaa jakaa käyttäjien klikkaamia linkkejä automaattisesti. RSS:n kieltäminen kiinnostaa luultavasti eniten paljon bloggaavia yrityksiä, eikä ole Halti Oy:n kannalta ajankohtainen. Turvallisista sivustoista varoittaminen on monien yrityksien kannalta ikävää, koska käyttäjät eivät välttämättä mene varoituksen jälkeen yrityksen verkkosivuille. Yrityksien työntekijöiden kannalta kaikista radikaalein asia voidaan katsoa olevan linkkien automaattinen jakaminen.

Linkkien automaattinen jakaminen toimii Dashin (2011) mukaan suurin piirtein näin: käyttäjä klikkaa esimerkiksi uutissivustolle vievää linkkiä Facebookissa ja hyväksyy sivuston sovelluksen asentamispyynnön. Asentamispyynnöstä voi kieltäytyä, mutta se tulee käyttäjälle joka kerta linkkejä klikatessa. Kun käyttäjä on kerran hyväksynyt asentamispyynnön, rupeaa sovellus jakamaan käyttäjän nimissä kaikkia uutisia mitä käyttäjä klikkailee uutissivustolla, vaikka Facebook olisi kiinni. Yritysten ja työntekijöiden tulee miettiä opinnäytetyön tekijän mielestä tässä esimerkiksi sitä, kuinka järkevää on yrityksen kannalta, että sen työntekijät alkavat tahtomattaan jakamaan linkkejä esimerkiksi spekulatiivisesti otsikoidusta uutisesta ”BBBB-Marikahenna kuumissa, ja järkyttävissä, seksiasennoissa”. Opinnäytetyön tekijän mielestä tällaisten asioiden vuoksi on entistä tärkeämpää tiedottaa Halti Oy:n työntekijöitä sosiaalisesta mediasta.

Virustorjuntaohjelmat mainitsevat ohjeet eivät ota huomioon, etteivät mobiililaitteille suunnatut virustorjuntaohjelmat välttämättä toimi kovin hyvin. Westin (2010) selittää, etteivät markkinoilla olevat virustorjuntaohjelmat suojaa viruksiksi määritellyiltä haittasovelluksilta vaan troijalaisiksi ja vakoiluohjelmiksi määritetyiltä haittasovelluksilta. Virustorjuntaohjelmat eivät myöskään tarjoa estoja nollapäivähyökkäyksiin tai mobiilikäyttöjärjestelmien kernelien vikojen hyväksikäyttämiseen. Westin (2010) painottaa, että virustorjuntaohjelma on vain markkinointitermi ja mobiililaitteiden käyttäjät voivat tällä hetkellä suojautua haittasovelluksilta parhaiten käyttämällä järkeä ladatessaan ja asentaessaan sovelluksia. Lisäksi, koska opinnäytetyöllä ei ole budjettia, voidaan työssä vain suositella virustorjuntaohjelmien lisäselvitystä tulevaisuudessa.

Mitkään ohjeistot eivät varoita siitä, että älypuhelimen tiedot voidaan varastaa myös pääsemällä siihen hetkellisesti fyysisesti kiinni. Krebs (2011) kertoo, että esimerkiksi lentokentillä olevilla julkisilla latauspisteillä voi mobiililaitteessa olevat tiedot automaattisesti kopioitua käyttäjän tietämättä varkaan tietokoneelle. Uhalta voi tosin suojautua helposti sammuttamalla puhelin ennen latausta.

Nixu-yhtiön tietoturva-asiantuntija mainitsee Lehdon (2011) artikkelissa lyhyesti mobiililaitteiden ajoitetun lukituksen huonon puolen: motivoitunut hyökkääjä saa esimerkiksi iPhonen suojakoodin auki pahimmillaan seitsemässä minuutissa. Amatöörivarkaat tuskin saavat suojakoodeja auki näin nopeasti, mutta silti lukituksen avaaminen korostaa etäpyyhintävalmiuden tärkeyttä. Suojakoodin avaaminen ei ilmeisesti poista matkapuhelimien IMEI-koodilla etälukitsemista.

Opinnäytetyön tekijän mielestä ohjeistot eivät myöskään varoita älypuhelimissa automaattisesti sisäänkirjautuvista sovelluksista. Tällaisia ovat esimerkiksi monet Facebook –sovellukset, jotka päästävät käyttäjän suoraan palvelun tilille. Tätä kautta varas voi päästä käsiksi työntekijän moniin yhteystietoihin ja tehdä kenties pilaa ja levittää perättömiä huhuja työntekijän yrityksestä. Näin sovellukset ovat myös alttiina perheenjäsenille ja ystäville.

3 Uuden metodin kehittely

Uutta metodia varten täytyy opinnäytetyön tekijän mielestä yhdistää nykyinen tieto, varautuminen lähitulevaisuuden uhkiin ja ennen kaikkea Halti Oy:n tarpeet. Nämä kaikki täytyy prosessoida, tässä tapauksessa Ojasalon, Moilasen ja Rintalahden (2009) ja Järvisen ja Järvisen (2004), tutkimus- ja kehittämistyön ohjeiden mukaisesti mielekkääksi kokonaisuudeksi. Päätavoitteena on luoda ohjeistosta mobiilikäyttäjille tietoa antava, helppolukuinen ja Halti Oy:n tarpeet kattava. Arvopohjana ohjeistolle ovat hyvät käytänteet, koska Halti Oy:llä ei ole aikaisempaa mobiilitietoturvaa koskevaa ohjeistoa, jossa linjattaisiin aiheeseen politiikat ja strategiat. Kaikesta tietoturvasta vastaava osasto on Halti Oy:ssä käytännössä kahden ihmisen IT-osasto. Tämä korostaa käyttäjien tiedon tärkeyttä entisestään. Ohjeisto on itsessään tietoturvan hallinnollinen suojausmenetelmä, joka esittelee käytännöllistä tietoa ja fyysisiä ja teknisiä suojausmenetelmiä. Ohjeiston tehtävänä on kaiken lisäksi kartoittaa Halti Oy:n aikaisempia toimia mobiililaitteiden elinkaaren aikana. Näihin toimiin ohjeisto ei välttämättä tuo mitään uutta.

Kuva 3: Älypuhelimien elinkaari

Miksi ylipäätään metodi artefakti Halti Oy:n mobiilitietoturvaa kehitettäessä? Mobiilitietoturvan kehittämiseen täytyi valita jokin lähestymistapa ja ohjeiston muokkaaminen vaikutti alusta alkaen selkeältä tavalta ja sai Halti Oy:n edustajien hyväksynnän. Yhdistettäessä mobiililaitteita koskevaan ohjeistoon älypuhelimien elinkaari ja tietoturva, täytyy miettiä miten ohjeistosta saa selkeän kokonaisuuden. Jäsentämällä ohjeisto osaksi kronologisiin vaiheisiin, siitä saadaan selkeä. Samalla seurataan Järvisen ja Järvisen (2004, 114) antamaa määritelmää metodille: metodi on joukko askelia, joita käytetään suorittamaan tehtävä, siirtymään alkutilasta lopputilaan. Lopputila on tässä tapauksessa Halti Oy:n mahdollisimman järkevä mobiilitietoturva.

Koska mitkään luvussa ”2.1 Aikaisemmat mobiilitietoturvaa koskevat metodit” mainituista tai ylipäätään tiedonhankinnassa esiin tulleista ohjeista eivät olleet kronologisia, saadaan uudesta ohjeistosta myös innovatiivinen. Toisaalta ohjeistoa ei voi laatia kokonaan kronologiseksi, sillä mobiililaitteen loppukäyttäjän täytyy noudattaa tiettyjä neuvoja koko laitteen olemassa olon ajan. Näin on myös sosiaalisen median ohjeissa.

Mobiililaitteita ja sosiaalista mediaa koskevat ohjeet ovat järkevää koota samaan ohjeistoon, koska kuten luvussa 2.1 todettiin, ovat monet käyttäjälle suunnatuista neuvoista samoja, koska uhkat ovat samoja. Monia mobiililaitteisiin kohdistuvia uhkia ei olisi ilman somea. Lisäksi molemmat aiheet, matkapuhelimet ja sosiaalinen media, ovat nousseet vahvasti olennaisiksi osiksi käyttäjiensä elämää melko samalla aikavälillä ja ovat käyttäjien avulla kasvavasti vuorovaikutuksessa toistensa kanssa (Smartphone Malware 2011; Kanalley 2011; Few Smartphone Owners Check In With Geosocial Services 2011).

Koska mobiililaitteiden elinkaaren kaikki vaiheet eivät koske loppukäyttäjää, voi ohjeiston jakaa kahteen osaan. Toinen osa mobiililaitteen esiasentajalle ja ylläpitäjälle, ja toinen loppukäyttäjälle. Näin käyttäjälle suunnatuista ohjeista saadaan lyhyempi ja pyritään noudattamaan Halti Oy:n edustajan neuvoa tehdä ohjeistosta lyhyt. Mobiililaitteista vastaavan IT-osaston täytyy kuitenkin lukea molemmat ohjeet. Mitä ohjeiston tulee sisältää? Seuraava luku kartoittaa tätä kysymystä lukijalle Halti Oy:n mobiililaitteiden käyttäjäryhmien kautta ja luku ”3.2 Metodin toimivuuden testaus ja konstruktion oikeellisuuden osoittaminen” esittää lukijalle perustelut ohjeistoon valituille ohjeille. Huomioitavaa on, että tässä opinnäytetyö poikkeaa periaatteessa Ojasalon, Moilasen ja Rintalahden (2009, 67) luettelemista konstruktiivisen tutkimuksen prosessin vaiheista, koska samanaikaisesti pyritään todistamaan konstruktion oikeellisuus ja teoriakytkennät. Periaatteessa oikeellisuutta ja teoriakytkentöjä on pyritty osoittamaan koko opinnäytetyön ajan.

3.1 Metodin teoreettiset ja empiiriset perustelut

Luvussa 2.2 päädyttiin siihen tulokseen, että mobiilitietoturvan ohjeiston on oltava mobiililaitteiden käyttäjille selkeä ja ottaa huomioon käyttäjien eri tarpeet. Seuraavissa kappaleissa käydään läpi Halti Oy:n käyttäjien tarpeita. Käyttäjien tarpeet luokitellaan sen mukaan, mihin Halti Oy:n tietoon heillä on mahdollisesti pääsy mobiililaitteellaan ja mitä riskejä niihin kohdistuu. Kaikki älypuhelimien käyttäjät käyttävät laitteita VAHTI:ssa (2007b, 15) mainitulla ”älypuhelimella käytetään hyvin rajoitetusti organisaation tietojärjestelmiä (esimerkiksi sähköposti)” -tavalla. Huomioitavaa siis on, ettei mobiililaitteilla oteta yhteyttä intranetiin tai käytetä VPN-tunnelointia. Tämä sulkee monia uhkia pois, mutta on toisaalta aihe johon on hyvä tutustua tulevaisuudessa. Mobiililaittesiin liittyvissä teknisissä suojaamismenetelmissä täytyy ottaa huomioon, että lähes kaikki Halti Oy:n puhelimet ovat Nokian E –sarjaa (2011b), joka tukee tiettyjä tietoturvaominaisuuksia.

Ensimmäinen, kaikista vaativin ja toisaalta myös pienin ryhmä ovat johtotehtävissä toimivat henkilöt. He matkustavat vuosittain monia kertoja Eurooppaan, Aasiaan, jne., käyttävät Nokian E-sarjan älypuhelinta koko ajan ja heillä on mahdollisesti mobiililaitteillaan/ mobiililaitteella auki olevassa sähköpostissa:

- sopimuksia kaikkien yrityksen sidosryhmien kanssa
- tieto yrityksen rahoista
- yrityksen johtoryhmän sisäisiä sähköposteja
- tietoa tulevista vaatemalleista
- yrityksen sisäisiä sähköposteja
- tärkeitä kontaktitietoja
- mahdollisesti jokin sosiaalisen median sovellus asennettuna
- henkilökohtaisia tietoja, kuten kuvia, talletettuja salasanoja
- automaattinen sisäänkirjautuminen yrityksen langattomaan verkkoon
- rajattomasti puheaikaa, tekstiviestejä ja tiedonsiirtokapasiteettia

Sähköpostit voivat vuotaa esimerkiksi seuraavilla tavoilla: älypuhelin varastetaan/katoaa tai sähköposti kaapataan nk. man in the middle –hyökkäyksellä, joko haittasovelluksen tai langattoman tiedonsiirron avulla. Ulkomailla täytyy ottaa huomioon, että eri maiden, kuten Ruotsin ja Kiinan, valtiot keräävät kaiken maahan tulevan ja maasta lähtevän Internetin välityksellä kulkevan tiedon. Tämä koskee myös salattuja sähköposteja, tosin jos salaus on tarpeeksi vahva, pitäisi tässä kulua kauan aikaa. Vaikkei tietyssä sopimuksessa sinänsä mitään arkaluontoista olisikaan, on sen vuotaminen selvästi epäluottamusta herättävää. Ryhmälle suositellaan otettavaksi käyttöön mahdollisimman paljon suojaamismenetelmiä. Toisaalta ryhmä käyttää älypuhelimiaan jatkuvasti, joten esimerkiksi lukituksen päälle laittaminen viiden minuutin toimettomuuden jälkeen ei ole vaihtoehto. Toinen johdon kaltainen ryhmä ovat työntekijät, jotka pitävät yllä suhteita yrityksen sidosryhmiin ja tarkkailevat laatua. He muistuttavat johtoa niin paljon ettei heitä kannata luokitella erikseen.

Toinen, vaativa ja johtoa suurempi ryhmä ovat myyjät/ulkomaalaiset myyjät. He matkustavat koko ajan Suomessa/ ulkomailla, käyttävät Nokian älypuhelinta koko ajan ja heillä on mahdollisesti mobiililaitteillaan/ mobiililaitteella auki olevassa sähköpostissa:

- sopimuksia yrityksen sidosryhmien kanssa
- rajoitetusti tietoa yrityksen rahoista
- tietoa tulevista vaatemalleista
- yrityksen sisäisiä sähköposteja
- tärkeitä kontaktitietoja
- mahdollisesti jokin sosiaalisen median sovellus asennettuna

- henkilökohtaisia tietoja, kuten kuvia, talletettuja salasanoja
- automaattinen sisäänkirjautuminen yrityksen langattomaan verkkoon
- rajattomasti puheaikaa, tekstiviestejä ja tiedonsiirtokapasiteettia

Vaikkei ryhmällä ole pääsyä yhtä tärkeään tietoon kuin johdolla, ovat he alttiimpia uhille matkustaessaan jatkuvasti. Puhelimen lukitus liian lyhyen ajan päästä ei vaihtoehto, vaikka siihen liittyvien uhkien todennäköisyys suurempi. Ulkomaalaisien myyjien vuoksi mobiilitietoturvaohjeiston on oltava myös englanninkielellä. Sitä lukevatko ulkomailla olevat myyjät ohjeistoa on myös vaikea seurata.

Kolmas ja isoin ryhmä ovat muut älypuhelinta käyttävät työntekijät. He saattavat matkustaa vuosittain ulkomaille, käyttävät Nokian älypuhelinta melko usein ja heillä on mahdollisesti mobiililaitteillaan/ mobiililaitteella auki olevassa sähköpostissa:

- tietoa tulevista vaatemalleista
- yrityksen sisäisiä sähköposteja
- tärkeitä kontaktitietoja
- mahdollisesti jokin sosiaalisen median sovellus asennettuna
- henkilökohtaisia tietoja, kuten kuvia, talletettuja salasanoja
- automaattinen sisäänkirjautuminen yrityksen langattomaan verkkoon
- rajattomasti puheaikaa, tekstiviestejä ja tiedonsiirtokapasiteettia

Tähän ryhmään voidaan lukea myös muita matkapuhelimia käyttävät työntekijät, ilman tietoa tulevista vaatemalleista tai sisäisistä sähköposteista. Näistä käyttäjistä suurimman osan puhelimiin voidaan asentaa sähköposti ja sovelluksia. Karjalainen ja Puhakainen (2011) painottavat, että tavallisella työntekijälläkin on todennäköisesti tärkeätä tietoa yrityksestä.

Halti Oy:n sähköpostien turvaaminen on moniulotteinen asia. Se on suurimmalle osalle mobiilikäyttäjiä pakollinen. Tietyt tekniset suojaamismenetelmät sopivat siihen hyvin, mutta vastaan tulee käyttäjien aktiivisuus ja salauspalveluiden hinta. Käyttäjän kannalta helpoin keino turvata sähköposti on etähallinta, mutta mitä jos etähallintaan pystyvä työntekijä ei ole töissä? Etähallinnasta täytyy myös ilmoittaa käyttäjille. Opinnäytetyön tekijä on varma, etteivät esimerkiksi Halti Oy:n myyjät suostu laitteen lukituksen viiden minuutin viiveeseen. Realistisempi lukitusaika on puoli tuntia. Myöskään sähköpostin asettaminen salasanaa kysyväksi ei ole mahdollista.

Tiedonsalauspalveluiden ja Internet-yhteyden salauspalveluiden mahdollinen käyttöönotto jätetään suoraan tulevaisuudessa selvitettäväksi. Käyttöönotto vaatisi uusien sovellusten asentamista, käyttäjien kouluttamista ja kenties rahaa budjetista. Tällä hetkellä opinnäytetyön tekijä ei koe tiedon etäurkkimisen olevan kovin suuri uhka, mutta tulevaisuudessa salauksen käyttöönottaminen sekä tietoon, että tiedon välitykseen voivat hyvinkin olla pakollisia. Näin on myös anti-virusohjelmien hankkimisessa.

Tärkeät kontaktitiedot saa varmuuskopioitua helposti Nokia PC/OVI Suitella. Ohjeistossa täytyy varmistaa, että käyttäjällä on tietokoneessaan asennettuna PC/OVI Suite ohjelma. Kaikilla käyttäjäryhmillä on käytännössä mahdollisuus sosiaalisen median palveluiden asentamiseen/niissä vierailemiseen, joten somen ohjeisiin on valittu näkökulmaksi Rinnan (2011) laatima lista yrityksen viidestä suurimmasta tietoturvauhasta. Aikaisemmin esitellyt valmiit somea koskevat ohjeet sopivat tähän hyvin.

Lähes kaikilla älypuhelimien käyttäjillä oleva mobiililaitteen automaattinen sisäänkirjautuminen yrityksen langattomaan verkkoon on sinänsä ongelmallinen, mutta tunkeutujan on kuitenkin ensin päästävä aivan Halti Oy:n tuntumaan ennen puhelimen/SIM-kortin lukitsemista. Myös matkapuhelimen lukitsemisaika hieman poistaa tätä ongelmaa. Halti Oy:lle tulee lisälasku puheluista, tekstiviesteistä ja tiedonsiirrosta vain, jos mobiililaite katoaa ulkomailla tai sillä tehdään kyseiset toimenpiteet maksullisiin palveluihin.

Opinnäytetyön tekijä kokee, että ohjeissa on mainittava myös paikannukseen liittyvät ongelmat ja kertoa Facebookin uusista ominaisuuksista. Mitään tärkeätä tietoa ei kannata siirtää mobiililaitteen muistiin, mutta toisaalta laite on luultavasti paremmin suojattu katoamiselta, kuin muistitikku. Edellisten lisäksi ohjeistossa täytyy painottaa salasanoja, langattoman tiedonsiirron vaaroja ja sovellusten kieltämistä tai ”suositellut” –listan kokoamista esimerkiksi yrityksen intranetiin. Näin siksi, että jos käyttäjän salasana paljastuu yhdessä Internet-palvelussa, se ei paljastu kaikissa. Langatonta tiedonsiirtoa painotetaan kaikissa luvussa 2.1 läpi käydyissä ohjeissa. Kuten aikaisemmin mainittiin, mobiililaitteiden haittasovellusten määrän on arvioitu kasvavan.

Opinnäytetyön tekijä valitsee ohjeiston pääkohdaksi sen, että älypuhelimet ovat aivan kuin kannettavia tietokoneita, joiden tietoturva käyttäjien on ymmärrettävä. Monissa kouluissa, kuten Laurea-ammattikorkeakoulussa (2005), on jo aikoja sitten kielletty omien ohjelmien asentaminen koulun omistamiin tietokoneisiin, mutta onko tilanne sama älypuhelimissa? Seuraavassa luvussa esitellään liitteenä olevan ohjeiston yhtymäkohdat aikaisempiin ohjeistoihin ja syyt tiettyjen asioiden valitsemiselle.

3.2 Konstruktion oikeellisuuden osoittaminen, teoriakytkennät ja toimivuuden testaus

IT-osaston osio mobiilitietoturvaohjeistosta:

1. Yksinkertaistettu VAHTI:n (2007b, 20-24) ensimmäinen ja toinen vaihe älypuhelimien elinkaaressa. Käyttäjien tarpeet huomioitu.
2. Laiterekisteri toteuttaa VAHTI:ssa (2007, 29) mainitun inventoinnin, Lehdon (2011) ennakointi suosituksen ja Viestintäviraston (2009, 3) IMEI-koodin keräämisen. Laitteen sarjanumero, IMEI-koodi, on oltava tiedossa, jotta laite voidaan lukita, vaikkei siinä olisi enää Halti Oy:n SIM-korttia tai Internet-yhteyttä.
3. Vain tarvittavien sovellusten asentaminen toteuttaa VAHTI:n (2007b, 26-27), Viestintäviraston (2009, 4) ja Lehdon (2011) antamia neuvoja. Lehdon (2011) mukaan Mail For Exchange on pakollinen etähallintaominaisuuksien käyttöönottamiselle.
4. VAHTI (2007b, 45-47) ja Lehto (2011) suosittelevat etähallinnan käyttöönottamista. Nokia (2011b) luettelee Mail For Exchangen avulla E-sarjansa käyttövalmiit ActiveSyncin ominaisuudet ja Lehto (2011) täydentää mitkä niistä ovat kolmansien osapuolien tarjoamia. Esim. etälukitus on 3. osapuolelta ostettava ominaisuus. Aikalukon asettaminen 30 minuuttiin johtuu havainnoinnin perusteella kerätystä tiedosta, mutta mikäli käyttäjät ovat valmiita pienentämään aikaa, olisi se hyvä. 30 minuuttia ei pitäisi häiritä työntekoa, mutta suojaa amatöörivarkailta ja esim. uteliailta ystäviltä, mikäli mobiililaite unohtuu jonnekin. Kts. luku 2.2.
5. Viestintävirasto (2009) kehottaa suoraan mobiililaitteen tietojen varmuuskopiointiin, VAHTI (2007b, 26-27) ohjelmien vakiointiin ja Lehto (2011) laitteen häviämisen ennakointiin. Lisäksi Mail For Exchange on helppo hakea Nokia OVI Storesta.
6. VAHTI (2007b, 30) mainitsee käyttäjien koulutuksen, muut ohjeet käyttäjän omatoimisen tutustumisen käyttöohjeisiin.
7. VAHTI (2007b, 31): ”Älypuhelin ei juuri poikkea työaseman elinkaarenhallinnan tästä osa-alueesta”.
8. Liittyy käyttäjälähtöisyyteen ja mobiilitietoturvan kehittämiseen, esim. PDCA-mallin avulla.

Tulevaisuus: VAHTI (2007b, 26; 42), Viestintävirasto (2009, 2-4), Lehto (2011) kehottavat lisäsuojaa antavien sovellusten asentamisen mobiililaitteisiin ja varomaan ylimääräisiä sovelluksia. Laurea (2007a) muistuttaa haittaohjelmilta suojautumisesta.

Käyttäjien osio mobiilitietoturvaohjeistuksesta:
Ensimmäisessä osiossa pyritään selittämään käyttäjille, mitä tietoturva tarkoittaa Tampereen Yliopiston (2009) mukaan, mitä mobiililaitteet ovat opinnäytetyön mukaan ja kerrotaan hieman älypuhelimiin liittyviä tilastoja CNCCS:n (Smartphone Malware 2011, 13) ja Halti Oy:n IT-spesialisti Tammiston tietojen pohjalta. Kuva on opinnäytetyöntekijän omatekemä.
Numeroitujen kohtien lähteet menevät näin:

1. Laurea (2007a), Lehto (2011), VAHTI (2007b, 42), Viestintävirasto (2009, 3) kehottavat kiinnittämään huomiota PIN-koodiin. Esimerkki on opinnäytetyöntekijän keksimä.
2. Mukailtu VAHTI:n (2010, 36) ja Laurean (2010) mukaan. Gmail (2011) esimerkkinä.
3. Laurea (2007a), VAHTI (2007b, 43), Viestintävirasto (2009, 4)
4. Viestintävirasto (2009) kehottaa suoraan mobiililaitteen tietojen varmuuskopiointiin, VAHTI (2007b, 26-27) ohjelmien vakiointiin ja Lehto (2011) laitteen häviämisen ennakointiin. Lisäksi Mail For Exchange on helppo hakea Nokia OVI Storesta.
5. Lehto (2011) suosittelee päivittämistä ja Westinin (2010) mukaan se suojaa viruksilta. Nokia (2011c) mainitsee puhelimien nopeutumisen ja akunkeston parantumisen.
6. VAHTI (2007b, 26), Viestintävirasto (2009, 4), Lehto (2011)
7. Laurea (2007a), Lehto (2011), VAHTI (2007b, 40) ja Viestintävirasto (2009, 3)
8. Halti Oy:lle saapui monia phishing -tyyppisiä sähköpostiviestejä työharjoittelun aikana ja opinnäytetyöntekijä kokee, että asiasta pitää vielä mainita.
9. Krebs (2011)
10. -
11. Lehto (2011) ja mukailtu Laurean (2007a) ohjeista
12. VAHTI (2007b, 30) ”helpdesk” ja käyttäjälähtöisyys

Katoamistapauksen ohjeet ovat mukailtu Laurealta (2007a). Lopun ”vinkki” on opinnäytetyöntekijältä.

Sosiaalisen median ohjeissa ensimmäinen kappale on mukailtu VAHTI:sta (2010, 36). Seuraava osio, mitä saa ja mitä ei saa puhua, on Tyynysniemeltä (2011) ja VAHTI:sta (2010, 36). Sitä seuraava kappale on koostettu Laurealta (2007b) ja VAHTISTA (2010, 36). Lyhennetyistä, joko tarkoituksella tai älypuhelimen näytön koon vuoksi, Internet-linkeistä varoittavat VAHTI (2010, 29) ja Dwivedi ym. (2010, 4). Sovellusten asentaminen liittyy VAHTI:in (2007b, 26), Viestintäviraston (2009, 4) ja Lehdon (2011) ohjeisiin. Lisäksi tähän kohtaan on sovellettu omia havaintoja. Paikannukseen liittyvät Frilander (2011), Kauppalehti (2011), Masalin (2011), Turun Sanomat (2011) ja VAHTI (2010, 32). Lopuksi muistutetaan somen palveluiden muutoksista Dashia (2011) mukaillen. Sosiaalisen median osiossa on otettu huomioon

VAHTI:ssa (2010, 28–29) annetut ohjeet ohjeistukseen ja koulutukseen, ja Rinnan (2011) listaamat yrityksen viisi suurinta sosiaalisen median tietoturvauhkaa.

Koko ohjeistossa on pyritty huomioimaan Karjalaisen ja Puhakaisen (2011) antamat ohjeet tietoturvakoulutuksesta ja otettu hieman mallia Viestintäviraston (2009) ohjeesta. Mikäli ohjeen lukija on kiinnostunut aiheesta, hänet on pyritty ohjaamaan opinnäytetyön pariin. Ohjeiston konkreettinen toimivuuden testaus tapahtuu vasta käytännössä, mutta opinnäytetyön osoittamassa teoriassa käyttöönotettujen suojaamismenetelmien avulla tietoturva on Halti Oy:lle järkevästi suojattu.

4 Keskustelu

Tosiasiana täytyy muistaa, että mikäli päättäväinen ja osaava varas haluaa murtautua ylipäänsä pienten, keskisuurien ja isojenkin suomalaisten yritysten tietojärjestelmiin, se onnistuu luultavasti tavalla tai toisella. MBnet (2011) uutisoi elokuussa historiallisesta nettimurtojen sarjasta, jossa McAfee tietoturvayhtiö arvioi olleen takana valtiotason toimija. Hyökkääjät onnistuivat esimerkiksi tarkkailemaan YK:n Geneven sihteeristön tietojärjestelmää lähes kahden vuoden ajan ja varastamaan mm. asekauppaan ja korkean teknologian yritysten tietoja. Yksittäiset valtiotkin hävittävät tietoja koko ajan: Harrison (2008) raportoi The Telegraph lehdessä, että vuonna 2007 Ison-Britannian valtio hävitti yhteensä 37 miljoonaa kappaletta henkilökohtaisia tietoja. Samassa artikkelissa Harrison (2008) kertoo, että keskimäärin 80 Ison-Britannian passia hukkuu kuukaudessa. Näissä asioissa pitää muistaa, että valtiollista toimijaa tuskin kiinnostaa liian pienien yritysten tiedot. Tietoturvassa ei ole kaikkien kohdalla kyse parhaasta mahdollisesta tietosuojasta, vaan kyseiselle toimijalle järkevimmästä.

Vain aika näyttää kuinka paljon mobiililaitteissa olevia tietoja ruvetaan urkkimaan suoraan langattoman tiedonsiirron avulla. Jos urkinta ja haittaohjelmat alkavat yleistymään, yrityksen tulisi olla samoin tein valmis aloittamaan seuraavat mobiilitietoturvan kehitysprosessit. Tulevaisuudessa on mahdollisuuksia myös ”positiivisiin” kehittämisprojekteihin, kuten esimerkiksi virtuaalisoinnin tehostamiseen tai kadonneiden mobiililaitteiden jäljitykseen GadgetTrakin (Photographer Recovers $9K Stolen Camera & Equipment Thanks to GadgetTrak 2011) avulla. Mobiilitietoturvaohjeistuksen kehittäminen eteenpäin jää Halti Oy:n harteille. Ohjeistusta voisi esimerkiksi viedä vielä teknisempään suuntaan ja kartoittaa aiheita tarkemmin. Mitään aiemmin mainittuja kehittämisprojekteja ennen, kannattaa kuitenkin miettiä virallisia politiikkoja ja suunnitella virallista strategiaa mobiilitietoturvan varalta.

Mikäli lukija haluaa itse testata kuinka helppoa ”hakkerointi” voi oikeastaan olla, voidaan hänelle suositella vuonna 2010 ilmestynyttä Firesheep –ohjelmaa ja 2011 elokuussa ilmestynyttä Android –puhelimen sovellusta nimeltään Android Network Toolkit (Anti). Firesheep (2010) on Firefox –selaimen lisäosa, joka demonstroi HTTP session kaappausta muutamalla klikkauksella. Pitkänen (2011) kertoo, että Anti skannaa älypuhelimen avulla lähialueen Wi-Fi-verkkoja, näyttää potentiaaliset kohteet ja tarjoaa eri hyökkäysvaihtoehtoja. Opinnäytetyöntekijä ei ole itse kokeillut kumpaakaan ohjelmaa, ei ota mitään vastuuta niiden toimivuudesta ja huomauttaa, että niiden käyttäminen ketään muuta kuin itseään ja omia järjestelmiä vastaan on laitonta.

4.1 Tulokset

Aikaisempiin ohjeistoihin ja lähdemateriaaliin verrattuna, opinnäytetyön tuloksena saatu ohjeisto on lähitulevaisuutta varten toimiva. Tämä on pyritty todistamaan aikaisemmissa luvuissa. Ohjeistoa voivat periaatteessa soveltaa myös muut yritykset, samoin kuin yksityishenkilöt. Sinänsä ohjeisto ei sisällä uutta tietoa globaalisti, vain uutta tietoa Halti Oy:lle. Toisaalta se yhdistää mobiililaitteita ja sosiaalista mediaa koskevat ohjeet samaan ohjeistoon tavalla, jota ei aikaisemmin ole ollut. Nämä asiat huomioiden opinnäytetyö täyttää Järvisen ja Järvisen (2004, 113-115) määritelmiä uudelle metodi -innovaatiolle: vanhaa yhdistämällä ollaan saatu uutta ja tutkimuksen tulos on sovellettavissa muihin tapauksiin. Ohjeisto saa toivottavasti edes osan Halti Oy:n työntekijöistä ajattelemaan älypuhelintaan muuna kuin normaalina matkapuhelimena. Yrityksen tietoturvasta vastaaville henkilöille ohjeisto ja opinnäytetyö antavat mietittävää tulevaisuutta varten.

4.2 Jälkipuhe

Metodi artefaktin konstruoiminen oli prosessi, jossa oppi uutta mm. prosesseista ja syvensi tietämystään erinäisistä asioista. Alunperäinen idea ohjeiston kokoamisesta vaikutti suhteellisen helpolta, mutta konstruktiivisen tutkimuksen kirjoittaminen opinnäytetyöprosessin syvetessä osoittautui paljon alun ajatuksia vaativammaksi. Alun paremmalla suunnittelulla olisi säästynyt huomattavalta vaivalta. Samoin olisi aiheen supistamisella. Halti Oy:lle olisi voinut esimerkiksi selvittää, minkälaisia tietoturvaohjeistoja on muilla ulkoiluvälineyrityksillä.

Oman tekstin tuottamiseen tarvittu aika oli yksi eniten yllättäneistä asioista opinnäytetyötä tehdessä, ja tämä rikkoi aikataulut toistensa perään. Suunnitellessa olisi pitänyt varautua pahimpaan. Toisaalta, kantapään kautta oppiminen näytti konkreettisesti kuinka opinnäytetyöprosessi eteni iteratiivisesti jotakuinkin näin:

Vaihe 1.
ONT idea: mobiilitietoturva
ONT alustava materiaaliin tutustuminen
ONT ideasta puhuminen ja hyväksyttäminen työharjoittelussa
Työn hahmottelu: auditointi ja auditoinnin perusteella ohjeistus
Aiheanalyysin tuottaminen

- Palaute ja ideointi –

Vaihe 2.
ONT: Mobiilitietoturva askel askeleelta -ohjeistus Halti Oy:lle
Auditointi pois
Puhuminen aiheesta yrityksessä ja tarkennetun aiheen hyväksyttäminen
Lähteiden monipuolistaminen; aktiivinen tutustuminen eri lähteiden materiaaliin ja suurimman lähdemateriaalimäärän kerääminen
Sisällysluettelon laatiminen muiden ONT:iden, insinöörityön ja lähdemateriaalin perusteella
Tutkimussuunnitelman tuottaminen

- Palaute ja ideointi -

Vaihe 3.
ONT:n täydellinen synkronointi konstruktiivisen tutkimuksen menetelmiin ja uuden it-artefaktin luomisprosessiin
Mobiilitietoturvaohjeistus it-artefakti, joka toimii opastavana metodina Halti Oy:n mobiilitietoturvan hyväksi
Lisää lähdemateriaalia
Valmiin opinnäytetyön tuottaminen

Opinnäytetyö kirkastui lisää jokaisessa vaiheessa, vaikka ideointi oli jatkuvasti käynnissä. Tämä oli työmäärän kannalta huono asia, mutta toisaalta pakotti koko ajan ajattelemaan mitä opinnäytetyössä pitää tehdä. Lisäksi melkein kaiken toisessa vaiheessa tuotetun materiaalin pystyi kuitenkin integroimaan opinnäytetyöhön, eikä materiaalin etsiminen mennyt missään vaiheessa hukkaan. Paljon materiaalia jäi tosin käyttämättä. Esimerkiksi mobiililaitteille suunnatut haittasovellukset jäivät käsittelemättä suorasti. Opinnäytetyön tekeminen mukaili paljolti Laurea-ammattikorkeakoulun opinnäytetyöprosessin vaiheita. Suurimmat eroavaisuudet ovat, että toteutusvaiheen työpajat suoritettiin jo orientaatiovaiheessa, eikä tutkimussuunnitelma ollut jälkikäteen katsottuna tarpeeksi mietitty.

Lähteet

Brodkin, J. 2011. Cisco: Facebook security more important as e-mail spam levels drop. Viitattu 14.11.2011. http://www.networkworld.com/news/2011/030111-demo-cisco-facebook-security.html?ap1=rcb

Butler, E. 2010. Firesheep. Viitattu 23.11.2011. http://codebutler.com/firesheep

Catanzariti, R. 2009. The Mobile Phone: A History in Pictures. Viitattu 15.09.2011. http://www.pcworld.com/article/172837/the_mobile_phone_a_history_in_pictures.html

Cellullar Subscribers 1990. 2004. Worldmapper. Viitattu 14.11.2011. http://www.worldmapper.org/display.php?selected=333

Dash, A. 2011. Facebook is gaslighting the web. We can fix it. Viitattu 23.11.2011. http://dashes.com/anil/2011/11/facebook-is-gaslighting-the-web.html

Data Loss Statistics. 2011. DataLossdb. Viitattu 20.11.2011. http://datalossdb.org/statistics?utf8=%E2%9C%93&timeframe=current_year

Domestic Manufacturers Cashing in on Smartphone Popularity. 2011. Asia Today. Viitattu 05.10.2011. http://asiatoday.com/pressrelease/domestic-manufacturers-cashing-smartphone-popularity

Dwivedi, H., Clark, C. & Thiel, D. 2010. Mobile Application Security. Yhdysvallat: McGraw-Hill.

Fildes, J. 2010. Symbian phone operating system goes open source. Viitattu 06.10.2011. http://news.bbc.co.uk/2/hi/technology/8496263.stm

Frilander, A. 2011. Valvooko tuttu isoveli sinunkin kännykkääsi?. Viitattu 12.10.2011. http://www.tietoviikko.fi/kaikki_uutiset/valvooko+tuttu+isoveli+sinunkin+kannykkaasi/a659093?s=bu_talouselama&fail=f

From the App Store. 2011. Apple Viitattu 20.10.2011. http://www.apple.com/iphone/from-the-app-store/

Gartner. 2011. Gartner Says Sales of Mobile Devices Grew 5.6 Percent in Third Quarter of 2011; Smartphone Sales Increased 42 Percent. Viitattu 21.11.2011. http://www.gartner.com/it/page.jsp?id=1848514

Gmail. 2011. Google. Viitattu 22.11.2011. www.gmail.com

Gorlenko, L. & Merrick, R. 2003. No Wires Attached: Usability Challenges in the Connected Mobile World. IBM Systems Journal. Vol. 42:2.

Grabham, D. 2010. Intel and Nokia merge Moblin and Maemo to form MeeGo. Viitattu 06.10.2011. http://www.techradar.com/news/phone-and-communications/mobile-phones/intel-and-nokia-merge-moblin-and-maemo-to-form-meego-670302

Harrison, D. 2011. Government's record year of data loss. Viitattu 24.11.2011. www.telegraph.co.uk/news/politics/1574687/Governments-record-year-of-data-loss.html

International Telecommunication Union. 2008. 2G/3G/4G. Viitattu 04.10.2011. http://www.itu.int/ITU-D/imt-2000/DocumentsIMT2000/What_really_3G.pdf

iPod touch. 2011. Apple. Viitattu 20.10.2011. http://www.apple.com/fi/ipodtouch/

Järvinen, P., Järvinen, A. 2004. Tutkimustyön metodeista. Suomi: Tampereen Yliopistopaino.

Kanalley, C. 2011. The Growth of Social Media (INFOGRAPHIC). Viitattu 20.11.2011. http://www.huffingtonpost.com/2011/09/01/growth-social-media-infographic_n_945256.html

Karjalainen, M., Puhakainen, P. 2011. Yritysten tulee tehostaa tietoturvakoulutusta. Helsingin Sanomat 18.11.2011. A1.

Kauppalehti. 2011. Yritysten paikannusmarkkinoissa tietoturvaongelmia. Viitattu 12.10.2011. http://www.kauppalehti.fi/5/i/yritykset/yritysuutiset/?oid=20110886729

Kielikone Oy. 2011. MOT-sanakirja. Viitattu 14.09.2011. http://mot.kielikone.fi.nelli.laurea.fi/mot/laurea/netmot.exe?motportal=80

Korpinen, J. 2008. Pienehkö sivistyssanakirja. Viitattu 14.08.2011. http://www.cs.tut.fi/~jkorpela/siv/laaja.html

Kotilainen, S. 2011. Varo Android-tuholaisia! Ongelma kasvaa räjähdysvauhtia. Viitattu 21.11.2011. http://www.tietokone.fi/uutiset/varo_android_tuholaisia_ongelma_kasvaa_rajahdysvauhtia

Krebs, B. 2011. Beware of Juice-Jacking. Viitattu 17.11.2011. http://krebsonsecurity.com/2011/08/beware-of-juice-jacking/

Laitila, T. 2011. Älypuhelinten myynti ohittaa peruspuhelimet vuonna 2015. Viitattu 10.10.2011. http://www.puhelinvertailu.com/uutiset.cfm/2011/08/26/alypuhelinten_myynti_ohittaa_peruspuhelimet_vuonna_2015

Laurea-ammattikorkeakoulu Tietohallinto. 2011. Laurea-ammattikorkeakoulun tietoverkon ja -järjestelmien käyttösäännöt 1.11.2005 alkaen. Viitattu 23.11.2011. http://www.laurea.fi/fi/IT-palvelut/kayttajatunnukset/Sivut/Opiskelijoiden-kayttosaannot.aspx

Laurea-ammattikorkeakoulu. 2007a. Matkapuhelimen suojaamien – pähkinänkuori. Viitattu 17.11.2011.https://intra.laurea.fi/intra/fi/05_it_palvelut/02_saannot_ja_tietoturva/01_saannot_ja_tietoturva/Matkapuhelimet/index.jsp

Laurea-ammattikorkeakoulua. 2007b. Tietoturva ja tekijänoikeudet sosiaalisessa mediassa. Viitattu 15.11.2011. https://intra.laurea.fi/intra/fi/05_it_palvelut/02_saannot_ja_tietoturva/01_saannot_ja_tietoturva/Sosiaalisen_median_tietoturva/index.jsp

Laurea-ammattikorkeakoulu. 2010. Käyttäjätunnukset ja salasanat. Viitattu 13.11.2011. https://intra.laurea.fi/intra/fi/05_it_palvelut/02_saannot_ja_tietoturva/01_saannot_ja_tietoturva/Kayttajatunnukset_ja_salasanat/index.jsp

Lehto, T. 2011. Mobiiliuhkat kuriin. Tietokone -lehti. 07/2011. 38-41.

Lehto, T. 2011. Älypuhelinten tietoturvassa on isoja eroja. Viitattu 17.11.2011. http://www.tietokone.fi/uutiset/alypuhelinten_tietoturvassa_on_isoja_eroja

Leino, K. 2011. Joka neljännellä suomalaisella on käytössään älypuhelin. Viitattu 14.11.2011. http://www.tns-gallup.fi/index.php?k=14714

Litchfield, S. 2010. Defining the Smartphone – part 1. Viitattu 14.09.2011. http://www.allaboutsymbian.com/features/item/Defining_the_Smartphone.php

MarketingProfs. 2011. Few Smartphone Owners Check In With Geosocial Services. Viitattu 14.11.2011. http://www.marketingprofs.com/charts/2011/5883/few-smartphone-owners-check-in-with-geosocial-services

Masalin, T. 2011. Näin hävität paikannustiedot iPhonesta. Viitattu 10.10.2011. http://www.tietokone.fi/uutiset/nain_havitat_paikannustiedot_iphonesta

MBnet. 2011. Historiallisten nettimurtojen sarja paljastui. Viitattu 24.11.2011. http://www.mbnet.fi/uutiset/?uutinen=3221

Microsoft. 2011. Nokia and Microsoft Announce Plans for a Broad Strategic Partnership to Build a New Global Mobile Ecosystem. Viitattu 06.10.2011. http://www.microsoft.com/presspass/press/2011/feb11/02-11partnership.mspx

Mobiililaajakaista. 2011. Mobiililaajakaista-vertailu. Viitattu 13.11.2011. http://www.mobiililaajakaista.com/

Mobile internet use nearing 50%. 2011. British Broadcasting Corporation (BBC). Viitattu. 25.09.2011. http://www.bbc.co.uk/news/technology-14731757

Mobile/Tablet Top Operating System Share Trend. 2011. Netmarketshare. Viitattu 20.10.2011. http://www.netmarketshare.com/operating-system-market-share.aspx?qprid=9&qpcustomb=1&qptimeframe=M&qpsp=130&qpnp=25

Nemey, C. 2011. 5 top social media security threats. Viitattu 14.11.2011. www.networkworld.com/news/2011/053111-social-media-security.html

Nokia Siemens Networks. 2010. Claro Brazil keeps the customer satisfied with 3G. Viitattu 05.10.2011. http://www.nokiasiemensnetworks.com/news-events/publications/unite-magazine-issue-8/claro-brazil-keeps-the-customer-satisfied-with-3g

Nokia. 2011a. About Symbian. Viitattu 06.10.2011. http://symbian.nokia.com/about/

Nokia. 2011b. Mail for Exchange Security Overview. Viitattu 23.11.2011. http://europe.nokia.com/PRODUCT_METADATA_0/Find_products/Nokia_for_Business/pdf/502202342_MfE_security_data_sheet_%20Feb_2011.pdf

Nokia. 2011c. Nokia-ohjelmistopäivitykset. Viitattu 14.11.2011. http://www.nokia.com/fi-fi/tuki/nokia-ohjelmistopaivitykset/

Ojasalo, K., Moilanen, T., Ritalahti, J. 2009. Kehittämistyön menetelmät. Suomi: WSOYpro.

Oracle. 2011. About Java for Mobile Devices. Viitattu 21.09.2011. http://www.oracle.com/technetwork/java/javame/javamobile/overview/about/index.html

Oxford University Press. 2011. Oxford Advanced Learner's Dictionary. Viitattu 15.09.2011. http://oald8.oxfordlearnersdictionaries.com/dictionary/mobile-device

Patil, B., Saifullah, Y., Faccin, S., Sreemanthula, S., Aravamudhan, L., Sharma, S., Mononen, S. 2003. IP in Wireless Networks. Yhdysvallat: Prentice Hall.

Photographer Recovers $9K Stolen Camera & Equipment Thanks to GadgetTrak . 2011. GadgetTrak. Viitattu 23.11.2011.
http://www.gadgettrak.com/blog/2011/08/24/photographer-recovers-9k-stolen-camera-equipment-thanks-to-gadgettrak/

Pitkänen, M. 2011. Android-sovellus muuttaa puhelimen yksinkertaiseksi hakkerointityökaluksi. Viitattu 25.11.2011.
http://www.puhelinvertailu.com/uutiset.cfm/2011/08/08/android-sovellus_muuttaa_puhelimen_yksinkertaiseksi_hakkerointityokaluksi

Research In Motion (RIM). 2011a. About Research In Motion. Viitattu 06.10.2011.
http://us.blackberry.com/company.jsp

Research In Motion (RIM). 2011b. BlackBerry App World. Viitattu 06.10.2011.
http://appworld.blackberry.com/webstore/featured/?recordsPerPage=100&lang=en#licenseRadio

Rinta, N. 2011. Windows Phone 7:n mahdollisuus pärjätä markkinoilla – tietoturva. Viitattu 18.08.2011.
http://www.mikropc.net/kaikki_uutiset/windows+phone+7n+mahdollisuus+parjata+markkinoilla++tietoturva/a665618

Rinta, N. 2011. Yrityksen viisi suurinta sosiaalisen median tietoturvauhkaa. Viitattu 24.11.2011. http://www.tietoviikko.fi/kaikki_uutiset/article635238.ece

Salakuuntelussa ryvettynyt News of the World lopetetaan. 2011. Helsingin Sanomat. Viitattu 20.11.2011.
http://www.hs.fi/ulkomaat/artikkeli/Salakuuntelukohussa+ryvettynyt+News+of+the+World+lopetetaan/1135267633055

Smartphone Malware. 2011. The National Cyber-Security Advisory Council (CNCCS). Viitattu 21.11.2011. http://press.pandasecurity.com/usa/wp-content/uploads/2011/06/CNCCS-Smartphone-Malware-Full-Report-Translated-06-7-11-FINAL.pdf

Stakes. 2006. Kehittämistyön menetelmiä, osa 2, tiedonhankinnan menetelmiä. Viitattu 11.07.2011. http://info.stakes.fi/NR/rdonlyres/A85FCBC1-72BC-40D1-AE15-28ED3DFCC870/0/menetelmatosa2.pdf

Symantec panostaa nyt mobiililaitteiden tietoturvaan. 2010. Viitattu 21.10.2011.
http://www.symantec.com/fi/fi/about/news/release/article.jsp?prid=20101109_01

Taito Oulu. 2006. Mobiililaitteet. Viitattu 21.10.2011.
http://www.ouka.fi/taito/tietopaketit/teema2/dokut/mobiililaitteet.htm

Talouselämä. 2011. Yksityisyyden hallinta Facebookissa? Ei kiinnosta pätkääkään. Viitattu: 15.10.2011.
http://www.talouselama.fi/uutiset/yksityisyyden+hallinta+facebookissa+ei+kiinnosta+patkaakaan/a659549

Tampereen teknillinen yliopisto. 2009. Tietoturvamekanismien yleisesittely. Viitattu 15.07.2011. http://sec.cs.tut.fi/maso/materiaali.php?id=26

Tolvanen, P. 2011. Käsitteet ojennukseen: sosiaalinen media ja sen älyvapaa rajattomuus. Viitattu 15.10.2011. http://vierityspalkki.fi/2011/05/24/kasitteet-ojennukseen-sosiaalinen-media-ja-sen-alyvapaa-rajattomuus/

Tomminen, J. 2011. Sertifikaattien ABC – mitä DigiNotar-murto merkitsee minulle? Viitattu 17.11.2011.
http://www.tietoviikko.fi/kaikki_uutiset/sertifikaattien+abc++mita+diginotarmurto+merkitsee+minulle/a683150

Turun Sanomat. 2011. Paikannusmarkkinointi huolestuttaa tietoturva-asiantuntijaa. Viitattu 12.10.2011. http://www.ts.fi/online/kotimaa/246792.html

Tuurala, A. 2011. Sosiaalisen median sankarit. Tietokone –lehti. 07/2011. 42-47.

Tyynysniemi, M. 2011. Työntekijä, suu kiinni!. Helsingin Sanomat 24.07.2011. C8.

Uusheimo, T. 1998. Nokia Communicator 9000(i). Viitattu 15.09.2011.
http://netti.nic.fi/~jmietti/pda/kommu.htm

Waisybabu. 2011. iPhone 4S CPU Clocked At 800MHz Is 73% Faster Than iPhone 4, Twice As Fast As Galaxy S II, And All Other Android Phones. Viitattu 14.11.2011.
http://www.redmondpie.com/iphone-4s-cpu-clocked-at-800mhz-is-73-faster-than-iphone-4-twice-as-fast-as-galaxy-s-ii-and-all-other-android-phones/

Valtionhallinnon tietoturvallisuuden johtoryhmä (VAHTI). 2007a. Tietoturvallisuudella tuloksia. Suomi: Edita Prima.

Valtionhallinnon tietoturvallisuuden johtoryhmä (VAHTI). 2007b. Älypuhelimien tietoturvallisuus – hyvät käytännöt. Viitattu 25.11.2011.
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20071120Aelypuh/name.jsp

Valtionhallinnon tietoturvallisuuden johtoryhmä (VAHTI). 2008. Valtionhallinnon tietoturvasanasto. Suomi: Edita Prima.

Westin, K. 2010. Mobile Anti-Virus Myth. Viitattu 17.11.2011.
http://www.gadgettrak.com/blog/2010/10/09/the-mobile-anti-virus-myth/

Viestintävirasto. 2009. Matkapuhelimen käyttäjän tietoturvaohje. Viitattu 15.11.2011.
http://www.ficora.fi/mobiiliturva/pdf/opas_www_fi.pdf

Kuva 1: International Telecommunication Union. 2008. 2G/3G/4G. Viitattu 21.11.2011. http://www.itu.int/ITU-D/imt-2000/Revised_JV/IntroducingIMT_item3.html

Kuva 2: Smartphone Malware. 2011. The National Cyber-Security Advisory Council (CNCCS). Viitattu 21.11.2011. http://press.pandasecurity.com/usa/wp-content/uploads/2011/06/CNCCS-Smartphone-Malware-Full-Report-Translated-06-7-11-FINAL.pdf

Kuva 3: Valtionhallinnon tietoturvallisuuden johtoryhmä (VAHTI). 2007b. Älypuhelimien tietoturvallisuus – hyvät käytännöt. Viitattu 24.11.2011. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20071120Aelypuh/name.jsp

Kuvat ja kuviot

Liitteet

11/2011

IT-osaston toimet mobiilitietoturvan hyväksi:

Seuraava ohjeistus on tarkoitettu Halti Oy:n mobiilitietoturvan varmistamiseksi. Ohjeistuksessa keskitytään Haltin kannalta olennaisiin mobiililaitteisiin, eli matka- ja älypuhelimiin.

1. **Käyttäjän tarpeiden kartoittaminen**
   Mihin käyttäjä tarvitsee puhelintaan, ja mihin ei. Onko yrityksellä jo valmiiksi vanhaa laitetta annettavaksi? Jos Internetiin ja sähköpostiin pääsy on välttämätöntä, kuinka tehokas puhelimen täytyy olla? On huomioitava, että laitteen tulee olla mieluummin liian tehokas kuin tehoton työtehtävää varten!

2. **Laiterekisteri**
   Uuden mobiililaitteen saapuessa siitä tulee kirjata tietokantaan sen sarjanumero, malli, käyttäjän nimi ja puhelinnumero. Näin yrityksen laitteistosta pysytään kirjoilla ja varkauden sattuessa poliisille voidaan ilmoittaa laitteen sarjanumero. Toisaalta, jos rekisteriä ei päivitetä ajanmukaisesti, on se turha. Nokian laitteiden sarjanumeron saa esiin syöttämällä niihin koodin *#06#.

3. **Puhelimen asentaminen**
   a. Puhelimen käyttöjärjestelmän päivittäminen Nokia Ovi Suiten tai PC Suiten kautta
   b. Mail For Exchange – sähköpostiohjelman asentaminen
   Tähän vaiheeseen tarvitaan käyttäjälle tarkoitettu SIM-kortti ja hänen sähköpostinsa salasana, jonka käyttäjä mielellään itse syöttää puhelimeen.

4. **ActiveSync -hallintatyökalun käyttöönottaminen, hallinnointi ja käyttäjien tiedottaminen**
   Microsoft Exchange -sähköpostipalvelimelta tulee ottaa käyttöön ActiveSync -hallintatyökalu, ja aktivoida sillä Nokian E-sarjan tukemat etäpyyhintä (remote wipe) ja laitteen aikalukko 30 minuuttia -ominaisuudet. Käyttäjiä pitää tiedottaa aikalukosta, ja mikäli palaute on negatiivista, sen käyttöönottamista miettiä uudelleen.
   ActiveSyncin hallinnointi: sähköpostipalvelin: Exchange System Manager: Global Settings: Mobile Services: Properties

5. **Nokia Ovi Suiten tai PC Suiten asentaminen käyttäjän tietokoneelle mikäli käyttäjä ei itse osaa**
   Mobiililaitteen käyttäjän on myös hyvä osata näiden ohjelmien perusteet, vähintään yhteystietojen varmuuskopiointi.

6. **Käyttäjää pitää informoida mobiililaitteen ominaisuuksista ja tietoturvasta**
   Käyttäjän on hyvä tietää, miten hän voi varmuuskopioida puhelimensa sisällön Nokia Ovi Suitella tai PC Suitella. Lisäksi käyttäjän on tiedettävä, miten hänen täytyy toimia, jos laite katoaa, menee rikki, sähköpostin salasana paljastuu, puhelimeen saapuu epäilyttäviä viestejä tai käyttäjä epäilee laitteensa tietoturvan vaarantuneen. Käyttäjälle on hyvä painottaa, että hänen tulee ottaa yhteyttä IT-tukeen, mikäli hän on epävarma jostain.

7. **Mobiililaite täytyy elinkaarensa lopuksi hävittää huolellisesti**
   Mobiililaite voi sisältää yrityksen kannalta tärkeätä tietoa muistissaan.

8. **IT-osaston kannattaa välillä kysyä palautetta ja kehitysehdotuksia mobiililaitteista, vaikkei virallista palautekyselyä järjestettäisikään.**

   Tulevaisuutta varten yrityksen tulee miettiä valmiuksia antivirus-, palomuuri-, ja salausohjelmien asentamisesta mobiililaitteisiin ja sovelluskauppojen kieltämistä tai sallituista sovelluksista tehtyä listaa yrityksen intranetiin. Tällä hetkellä laitteiston fyysisen turvallisuuden voidaan katsoa olevan vielä tietoturvan kannalta yrityksen tärkein huoli. Mobiililaitteiston suosion vain kasvaessa, tehojen noustessa ja niiden tehtävien monipuolistuessa ovat ne entistä houkuttelevampia kohteita haittaohjelmistojen tekijöille ja tiedon nuuskijoille.

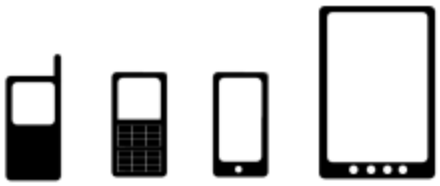
   Lisätietoja ja käytetyt lähteet löytyvät opinnäytetyöstä ”Mobiilitietoturvan kehittäminen Halti Oy:ssä ohjeiston avulla”.

Liite 1: IT-osaston toimet mobiilitietoturvan hyväksi

11/2011

Tietoturva

tarkoittaa tiivistetysti tiedon luottamuksellisuuden (tietoon on pääsy vain niillä, joille se on tarkoitettu), eheyden (tieto ei ole muuttunut luvattoman käsittelyn, siirron tai tallennuksen aikana) ja käytettävyyden (tieto on käytettävissä, kun sitä tarvitaan) turvaamista. Tietoturvauhalla tarkoitetaan uhkaa (esim. virus tai tietomurto), joka vaarantaa jonkin edellä mainitun tiedon osa-alueen. Tietoturvariskillä viitataan todennäköisyyteen, jolla tietoturvauhka toteutuu. Tietoturvan suojaamismenetelmät voidaan luokitella kolmeen kategoriaan: tekniset, fyysiset ja hallinnolliset menetelmät. Tekniset menetelmät tarkoittavat laitteistojen ja ohjelmistojen tietoturvaratkaisuja. Esimerkiksi palomuuri on tekninen menetelmä. Fyysiset menetelmät tarkoittavat esimerkiksi ovien lukitsemista ja paloturvallisuuden varmistamista. Yhtä hallinnollista menetelmää luet juuri nyt.



Mobiililaite tarkoittaa matkapuhelinta, älypuhelinta, kämmenmikroa, kameraa, jne.. Nykyään se voi tarkoittaa myös sormitietokonetta (iPad yms.). Seuraavassa termiä käytetään viittamaan matka- ja älypuhelimiin.

Ajattele älypuhelinta mieluummin kannettavana tietokoneena, kuin matkapuhelimena; älypuhelimien ominaisuudet ovat jo vanhojen kannettavien tietokoneiden tasolla ja kehittyvät entisestään. Tällä hetkellä tietokoneille tiedetään yli 60 miljoonaa haittaohjelmaa (viruksia, vakoiluohjelmia, troijalaisia, matoja, jne.). Älypuhelimille näitä tiedetään n. 600, mutta asiantuntijat odottavat älypuhelimille suunnattujen haittaohjelmien määrän kasvavan jyrkästi. Lisäksi älypuhelin katoaa ja menee tietokonetta helpommin rikki. Katoaminen ja rikkoutuminen ovat itse asiassa haittaohjelmia todennäköisempiä älypuhelimien tuhoajia. Lue siis seuraavat ohjeet, jotka tarjoavat helpot keinot auttaa yritystäsi ja itseäsi:

1. **PIN**
   Puhelimen PIN –koodi kannattaa vaihtaa edes muotoon 13579. Tämä koodi on joka toinen numero yhdeksään saakka. Se on helposti arvattava, mutta helppo muistaa ja turvallisempi kuin 1234 tai 0000.

2. **Salasana**
   Laadi turvallinen salasana, eli sellainen joka sisältää vähintään kahdeksan merkkiä, isoja kirjaimia ja numeroita. Esim.: VIHREA.K01r4, kämnykk4, mies68amerikka. Laadi myös vähintään työsähköpostiin, vapaa-ajan sähköpostiin ja sosiaalisen media palveluihin omat salasanansa. Jos sinulla on vaikeuksia muistaa salasanasi, voit muodostaa työsähköpostin salasanan laittamalla vapaa-ajan sähköpostin salasanan eteen ja taakse numeron. Esim. 1mies68amerikka2. Esimerkiksi Googlen Gmailin salasanaa vaihtaessa näet suoraan minkä vahvuinen salasana on.

3. **Aseta puhelimesi Bluetooth, infrapuna ja langattomien verkkojen etsintä pois päältä, kun et tarvitse niitä**
   Uhille altistamisen lisäksi nämä toiminnot kuluttavat turhaan akkua.

4. **Varmuuskopioi Nokia Ovi Suitella tai PC Suitella vähintään yhteystietosi**
   Varmuuskopiointi säästää paljolta pään vaivalta ja on helppoa tehdä. Mikäli et osaa käyttää Nokia Ovi Suitea tai PC Suitea, lue niiden käyttöohjeet tai pyydä opastusta IT-tuesta.

5. **Päivitä mobiililaitteesi ohjelmisto**
   Pidä laitteesi ohjelmisto ajan tasalla tarkistamalla päivitykset Ovi tai PC Suitella. Muista varmuuskopioida puhelimesi, sillä päivittäminen saattaa poistaa sen kaikki tiedot. Päivittäminen voi nopeuttaa puhelimen toimintaa, nostaa akunkestoa ja sulkea tietoturva-aukkoja.

6. **Älä asenna työpuhelimeen ylimääräisiä sovelluksia**
   Vaikka älypuhelin tarjoaa paljon mahdollisuuksia uusiin sovelluksiin, on kyseessä kuitenkin työpuhelin, jonka sovellukset voivat altistaa tietoturvauhille. Sovellusten asentamista kannattaa miettiä vapaa-ajan puhelimessakin. Mieti myös, tarvitsetko välttämättä verkkopankkia aina mukanasi? Mikäli haluat kuitenkin asentaa sovelluksia, tee se Nokian Ovi Storen kautta, mielellään suosituimmista vaihtoehdoista, joilla on valmiiksi paljon lataajia.

7. **Mieti kuinka tärkeitä tiedostoja haluat mobiililaitteessasi säilyttää**
   Mitä vähemmän tietoa, sen vähemmän murheita.

8. **Muista ettei pankkisi kysy tilisi tietoja koskaan soittaen sinulle tai sähköpostilla**

9. **Sammuta mobiililaite yleisillä akunlatauspisteillä ja käytä ulkomailla omaa laturia**
   Ei ole tavatonta, että yleisiin akunlatauspisteisiin on liitetty tietokone, joka on asetettu lataamaan koko mobiililaitteen sisältö USB:n tai muun tiedonsiirtoväylän kautta. Sammuttaminen hankaloittaa myös varkaiden työtä.

10. **Lue vielä sosiaalista mediaa koskevat ohjeet**
    Ohjeissa on hyödyllistä lainopillista tietoa Suomesta.

11. **Mieti, mitä teet jos: laitteesi katoaa? laiteesi hajoaa? sähköpostin salasana paljastuu? laite on huono?**

12. **Epäselvissä tilanteissa ota yhteys IT-tukeen**
    IT-osasto on varmasti aina valmis auttamaan ongelmatilanteissa.

Ohjeet katoamistapauksessa

1. Ota yhteys operaattoriin ja sen jälkeen toimistotunteina IT-spesialisti Joonas Tammistoon. On tärkeää, että liittymäsi suljetaan ja salasanasi nollataan mahdollisimman pian katoamisen jälkeen. Puhelimelta voidaan myös pyyhkiä tiedot etähallinnan avulla. Selvitä IT-tukeen myös se, kuinka tärkeitä sähköposteja ja tallennettuja tiedostoja puhelimessa oli.

2. Jos olet asentanut mobiililaitteeseen pankkitilin hallintaohjelman tai asioinut sillä pankissasi, ota yhteys pankkiisi.

3. Mikäli työsähköpostisi salasana on sama kuin vapaa-ajan sähköpostisi ja/tai sosiaalisen median (Facebook), vaihda näiden salasanat mahdollisimman nopeasti.

4. Mikäli katoamisessa on epäily rikoksesta, ilmoita asiasta poliisille.

Vinkki

Pidä operaattorin ja IT-tuen ajan tasalla olevat puhelinnumerot ja sähköpostiosoitteet ylhäällä vapaa-ajan sähköpostisi luonnoksissa, jolloin pääset niihin käsiksi missä tahansa missä on Internet. Huomioitavaa on, että puhelimen yhteystietojen varmuuskopiotiedosto on kätevä edellä mainitun sähköpostin liitetiedostona, mutta suojaamattomana se voi paljastaa yhteystietosi kovin helposti

Lisätietoja ja käytetyt lähteet löytyvät opinnäytetyöstä ”Mobiilitietoturvan kehittäminen Halti Oy:ssä ohjeiston avulla”.

Liite 2: Käyttäjän toimet mobiilitietoturvan hyväksi

11/2011

Älä hölmöile. Kunnioita muita ihmisiä. Siinä on tiivistetysti sosiaalisen median käyttösäännöt niin töihin kuin vapaa-aikaan. Huomioi, että olet lähes väistämättä työpaikkasi (epävirallinen) edustaja sosiaalisen median palveluissa, joten sinulla on vastuu kirjoituksistasi myös työnantajallesi. Kirjoituksesi saattaa päätyä väärään paikkaan, vaikka luulisit kirjoittavasi vain ystävillesi. Seuraavassa suuntaviivat siihen mistä puhua Internetissä ja mistä ei:

Pitäisi voida puhua:

Työsuhteen ehdot, kuten palkka

Lomat ja vapaat (kerro lomamatkastasi kaukomaille mieluummin vasta matkan jälkeen)

Rajatapauksia:

Työnantajalle kielteisten tosiasioiden kertominen tai työn julkinen kommentoiminen ylipäänsä

Voimakkaat mielipiteet. Huomioi myös äärimielipiteitä ilmaiseviin ryhmiin kuuluminen

Älä puhu:

Pomon haukkuminen ja työnantajaa vahingoittavat puheet

Liikesalaisuudet

Lisäksi:

Mieti, mitä tietoja, niin itsestäsi kuin muista ihmisistä, laitat Internetiin

Onko vieraiden ihmisten välttämätöntä tietää missä työskentelet ja missä asut? Ystäviesi pitäisi tietää nämä jo. Henkilökohtaisten tietojen julkaisemisessa on aina olemassa riskinsä, eivätkä yksityiskohtaiset henkilötiedot ole esim. Facebookkiin liittymisen kannalta pakollisia. Tähän liittyen: älä hyväksy tuntemattomien ihmisten kaveripyyntöjä.

Mieti, mitä sovelluksia käytät ja asennat, ja mitä linkkejä klikkaat

Haittaohjelmat saattavat lähettää ystäviesi nimissä ”hauskoja, pakko katsoa” -linkkejä. Jos muut ystäväsi ovat kommentoineet linkkiä, se on luultavasti turvallinen.

Mieti, tarvitsetko todella Facebookkia tms. puhelimessasi

Älypuhelimet ovat helpompia hukata kuin tavalliset matkapuhelimet, koska ne ovat houkuttelevampia kohteita varkaille. Ilman esim. Facebook -sovellusta on häviämistilanteessa yksi huoli vähemmän. Lisäksi hölmön mielipiteen julkaiseminen koko maailmalle, esimerkiksi juhliessa, on askeleen kauempana. Jos kiusaus jonkin sosiaalisen median palvelun käyttämiseen kuitenkin on liian suuri, aseta palvelu aina kysymään salasanaa.

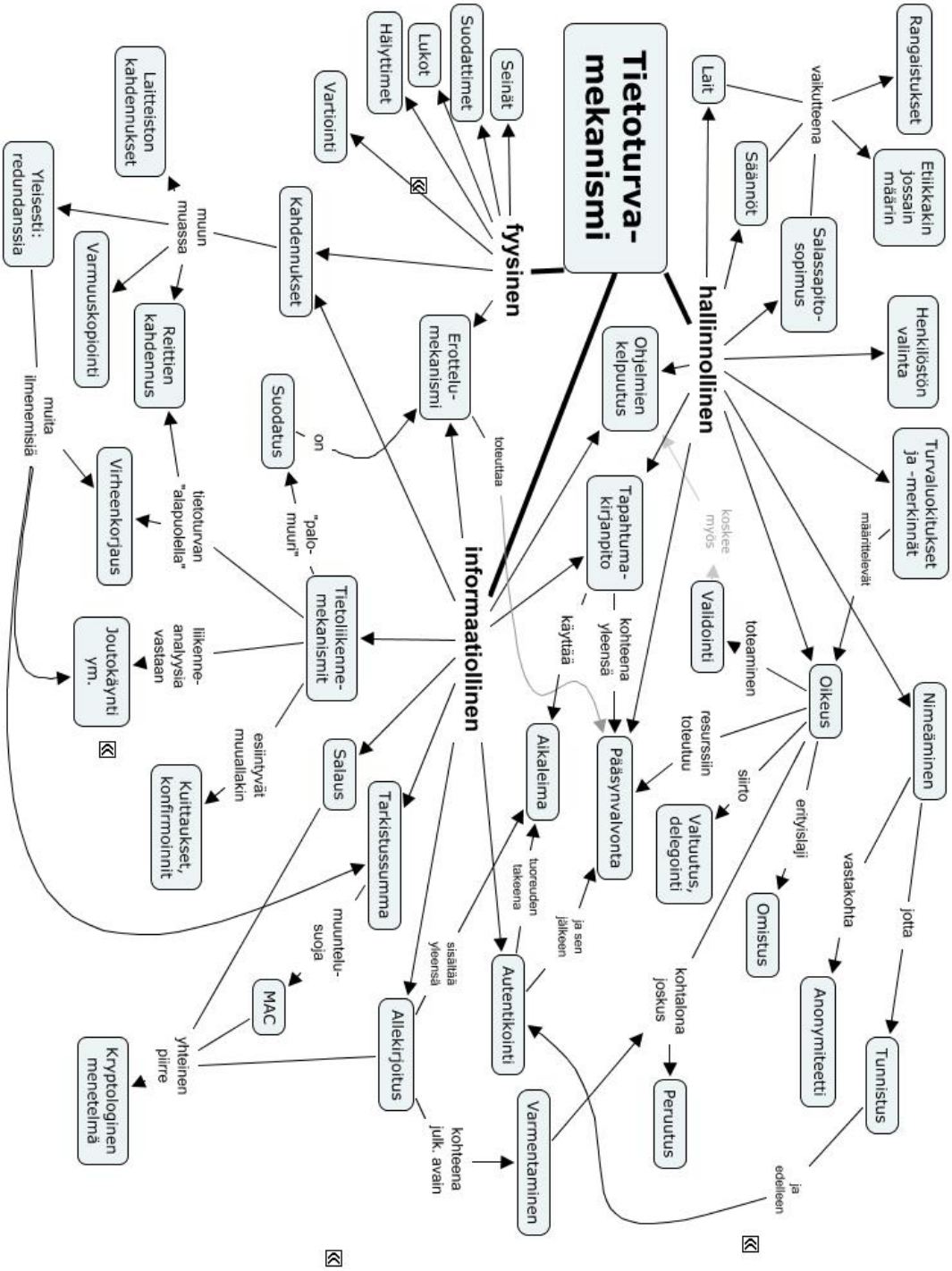
Mieti, haluatko antaa sovelluksien nähdä missä olet

Älypuhelimien sovellukset saattavat luovuttaa paikannustietojasi mainostajille; asuntosi saatetaan ryöstää lomalla ollessasi, vaikka jakaisit paikannustietosi vain ystävien kesken; voit jäädä kiinni valehtelemisesta tai sopimattomista paikoista; etc.. Huomio paikannus myös valokuvissa, sillä esim. iPhone tallentaa sillä otettuihin kuviin automaattisesti missä kuva on otettu!

Ota myös huomioon sosiaalisen median palveluiden jatkuvat muutokset!

Esimerkiksi Facebook otti juuri käyttöönsä ominaisuuden, jonka avulla käyttäjät jakavat tiettyjen uutispalveluiden sovelluksen asennuksen jälkeen automaattisesti käyttäjien klikkaamia uutisia sivustoilla. Ominaisuus toimii vaikka Facebook olisi kiinni.

Liite 3: Sosiaalisen median palveluiden ohjeet



Liite 4: Tietoturvamekanismien esittely